VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA STROJNÍHO INŽENÝRSTVÍ

LETECKÝ ÚSTAV

FACULTY OF MECHANICAL ENGINEERING

*INSTITUTE OF AEROSPACE ENGINEERING*

# VYUŽITÍ INFORMAČNÍCH TECHNOLOGIÍ PRO PODPORU SAFETY MANAGEMENTU V LETECTVÍ

THE USE OF INFORMATION TECHNOLOGY TO SUPPORT SAFETY MANAGEMENT IN AVIATION

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE — Bc. GABRIEL POLOCH

AUTHOR

VEDOUCÍ PRÁCE — Ing. MIROSLAV ŠPLÍCHAL, Ph.D.

SUPERVISOR

BRNO 2015

Vysoké učení technické v Brně, Fakulta strojního inženýrství

Letecký ústav
Akademický rok: 2014/2015

# ZADÁNÍ DIPLOMOVÉ PRÁCE

student(ka): Bc. Gabriel Poloch

který/která studuje v **magisterském navazujícím studijním programu**

obor: **Letecký provoz (3708T011)**

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách a se Studijním a zkušebním řádem VUT v Brně určuje následující téma diplomové práce:

**Využití informačních technologií pro podporu safety managementu v letectví**

v anglickém jazyce:

**The use of information technology to support safety management in aviation**

Stručná charakteristika problematiky úkolu:

Systémy řízení bezpečnosti se stávají součástí všech organizací, které působí v civilním letectví. Přes nepochybný přínos ve zvýšení bezpečnosti se zejména malé organizace musí vypořádat s nárustem agendy spojené s implemetací těchto systémů. Úkolem této práce je najít hvodné informační technologie, které mohou být pro takovéto organizace přínosné.

Cíle diplomové práce:

Cílem této práce je provést identifikaci softwarových nástrojů, které mají potenciál usnadnit implementaci systému řízení bezpečnosti v malých organizacích, které působí v civilním letectvím. Součástí úkolu je provést modelovou aplikaci zvoleného nástroje na schválenou organizaci pro výcvik (ATO) se složitou organizací.

Seznam odborné literatury:

[1] FAA: Introduction to Safety Management Systems to Air Operators. AC 120-92, 22.6.2006
[2] ŠALANDA, M. Zavedení systému řízení bezpečnosti u malého leteckého dopravce. Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2008. 58 s. Vedoucí diplomové práce Ing. Ondřej Schaumann
[3] ICAO. Doc 9422 ICAO Accident Prevention Programme. 2005

Vedoucí diplomové práce: Ing. Miroslav Šplíchal, Ph.D.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2014/2015.

V Brně, dne 24.11.2014

L.S.

| | |
|---|---|
| doc. Ing. Jaroslav Juračka, Ph.D.<br>Ředitel ústavu | doc. Ing. Jaroslav Katolický, Ph.D.<br>Děkan fakulty |

## ABSTRAKT

Úkolem této diplomové práce je seznámit čtenáře se Safety management systémem neboli se systémem řízení bezpečnosti. Práce se na počátku věnuje počátkům řízení bezpečnosti, důvodům proč takový systém vůbec vznikl a jaký byl jeho vývoj v minulosti. Stěžejní částí práce je identifikovat softwarové nástroje, jež by usnadnily implementaci Systému řízení bezpečnosti v organizacích pro výcvik. Součástí práce je také aplikovat zvolené softwarové nástroje na malou organizaci pro výcvik se složitou organizací.



**Klíčová slova**

Safety management systém, SMS, řízení bezpečnosti, řízení rizik, řízení kvality, malá organizace, letectví, ATO



## Abstract

The purpose of the Thesis is to acquaint reader with Safety management system in the aviation. In the beggining Thesis describes the begining of safety management, why was the system created and how it developed in the past. The main part of the Thesis is focused on identification of software tools for easier implementation of Safety management system in the training organizations. Another part of the Thesis is focused on aplication of selected software tools on small training organization (ATO) with complex disposition.



**Keywords**

Safety management system, SMS, Safety management, risk management, quality management, small organization, aviation, ATO

## BIBLIOGRAFICKÁ CITACE

POLOCH, G. Využití informačních technologií pro podporu safety managementu v letectví. Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2015. 56 s. Vedoucí diplomové práce Ing. Miroslav Šplíchal, Ph.D.

# ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že jsem byl seznámen s předpisy pro vypracování diplomové práce, a že jsem celou diplomovou práci vypracoval samostatně s použitím uvedené literatury a pod vedením vedoucího diplomové práce, Ing. Miroslava Šplíchala, Ph.D.

V Brně dne 29. 05. 2015 ……

Bc. Gabriel Poloch

# PODĚKOVÁNÍ

Na tomto místě bych rád poděkoval především vedoucímu mé diplomové práce panu Ing. Miroslavu Šplíchalovi, Ph.D. za vedení a odbornou pomoc a cenné připomínky při psaní této práce.

# OBSAH


**1 ÚVOD ..... 10**

**2 BEZPEČNOST ..... 11**

**3 DOKUMENTY ZABÝVAJÍCÍ SE SMS ..... 13**

**4 VÝVOJ BEZPEČNOSTI V LETECTVÍ ..... 15**

4.1 TECHNICKÉ OBDOBÍ ..... 15

4.2 OBDOBÍ LIDSKÉHO FAKTORU ..... 15

4.2.2 Reasonův model ..... 17

4.3 OBDOBÍ ORGANIZAČNÍ ..... 17

**5 BEZPEČNOSTNÍ KULTURA ORGANIZACE PROVOZOVATELE ..... 19**

**6 STRUKTURA IMPLEMENTACE SMS ..... 21**

6.1 POLITIKA A ZÁMĚRY/CÍLE BEZPEČNOSTI ..... 21

6.1.1 Závazek a odpovědnost vedení ..... 21

6.1.2 Odpovědnosti za bezpečnost ..... 22

6.1.3 Jmenování klíčového personálu ve vztahu k bezpečnosti ..... 22

6.1.4 Koordinace plánu reakce na nouzové situace ..... 22

6.1.5 SMS dokumentace ..... 22

6.2 ŘÍZENÍ BEZPEČNOSTNÍHO RIZIKA ..... 23

6.2.1 Zjišťování/identifikace nebezpečí ..... 24

6.2.1.1 Metody zjišťování / identifikace nebezpečí ..... 24

6.2.1.2 Zdroje zjišťování / identifikace nebezpečí ..... 25

6.2.2 Vyhodnocení a zmírnění rizika ..... 26

6.2.2.1 Proces vyhodnocení rizika ..... 26

6.2.2.2 Zmírnění bezpečnostního rizika/ kontrola ..... 28

6.2.2.3 Záznam o nebezpečích ..... 28

6.3 OVĚŘOVÁNÍ ÚROVNĚ BEZPEČNOSTI ..... 28

6.3.1 Sledování, hodnocení a průběžné zdokonalování výkonnosti v bezpečnosti ..... 29

6.3.2 Řízení změn ..... 30

6.4 PODPORA BEZPEČNOSTI ..... 30

6.4.1 Bezpečnostní výcvik ..... 30

6.4.2 Bezpečnostní komunikace ..... 32

**7 ROZBOR NABÍZENÝCH SOFTWAROVÝCH NÁSTROJŮ ..... 33**

7.1 SMS PRO ..... 33

7.2 AQD – AVIATION QUALITY DATABASE ..... 37

7.3 Q-PULSE ..... 41

7.4 ETQ ..... 44

7.5 INTELEX ..... 45

**8 MODELOVÁ APLIKACE ..... 48**

8.1 POLITIKA A ZÁMĚRY/CÍLE BEZPEČNOSTI ..... 49
8.2 ŘÍZENÍ BEZPEČNOSTNÍHO RIZIKA ..... 49
8.3 OVĚŘOVÁNÍ ÚROVNĚ BEZPEČNOSTI ..... 49
8.4 PODPORA BEZPEČNOSTI ..... 50
**ZÁVĚR ..... 51**
**SEZNAM POUŽITÉ LITERATURY ..... 52**
**SEZNAM OBRÁZKŮ ..... 54**
**SEZNAM TABULEK ..... 55**

# 1 ÚVOD

Letecká doprava se stále pyšní přívlastkem nejbezpečnější dopravní prostředek. Tohle je jistě pravda, protože navíc podle meziročních statistik stále ubývá počet úmrtí způsobených leteckou přepravou. Tyto úbytky jsou hlavně díky stále většímu- se věnování se kontrole a řízení bezpečnosti.

V počátcích letectví byla většina nehod zapříčiněna nevhodným či nedostatečným technickým stavem letecké techniky. S tímto souvisí první věnování se řízení bezpečnosti, které se zaměřovalo právě na dokonalost letecké techniky. S postupným zvýšením úrovně letecké techniky se dále zjistilo, že za největší počet leteckých nehod mohou právě lidé. Člověk je po všech stránkách nedokonalý a při své činnosti činí spousty chyb. V letecké dopravě se nehledí na člověka pouze jako na pilota, jenž během manévrů může způsobit nejvíce chyb. Pojem lidský činitel v letecké dopravě zahrnuje všechny, kdo se podílejí na provozu, od návrhářů letadel, přes letecké mechaniky, až po zmiňované piloty. Na člověka se v otázce bezpečnosti hledí právě proto, že jeho chybou vzniká až sedmdesát procent leteckých nehod.

S postupem času a v souvislosti se všemi činnostmi v letectví se zavedl pojem Safety management system, neboli Systém řízení bezpečnosti. Ten se věnuje všem problémům v letectví v otázce bezpečnosti. Systém řízení bezpečnosti musí v dnešní době být součástí všech společností věnujících se letecké dopravě.

Díky této povinnosti přibyla všem leteckým společnostem spousta práce. Společnosti často již mají ve svých postupech začleněný systém řízení bezpečnosti, ale mnohé z nich, především ty menší pouze v papírové podobě, což znamená spoustu papírů a složek a velice složitý systém.

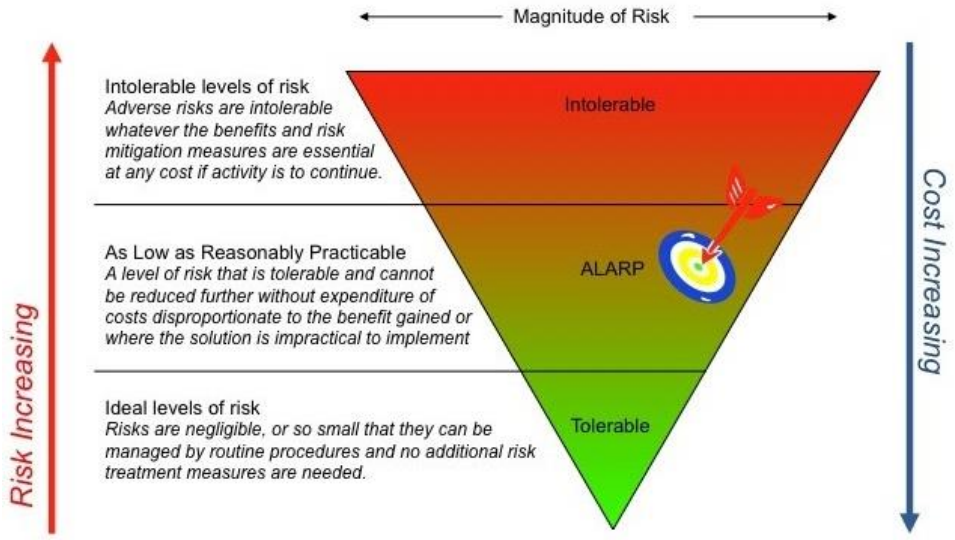
Na tuto situaci reaguje tato diplomová práce, jejímž tématem je prozkoumání a nalezení softwarových nástrojů pro usnadnění řízení implementací systému řízení bezpečnosti v malých organizacích, působících v civilním letectví. Součástí práce by také měla být modelová situace zvolených softwarových nástrojů na organizaci pro výcvik se složitou organizací.

# 2 BEZPEČNOST

**Systém řízení bezpečnosti** – SMS – představuje aktivní a systematický přístup k provozní bezpečnosti a jeho primárním účelem je zvyšovat bezpečnost. Systematicky vyhledává možná rizika a snižuje následky rizik již identifikovaných, jejichž důsledkem by mohlo být zranění osob nebo poškození majetku. Pro zvyšování bezpečnosti se používají tři systémy řízení bezpečnosti: systémový, pro-aktivní a explicitní.

**Bezpečnost** – je stav, kdy pravděpodobnost poškození majetku nebo újmy na zdraví osob je eliminována alespoň na minimální požadovanou úroveň. Toto je zajištěno průběžnou identifikací nebezpečí a řízením bezpečnostního rizika. [2]

Hlavním cílem SMS stále zůstává eliminace leteckých nehod a vážných incidentů, spojených s poškozením majetku a úrazy osob. Lidskou činností a činností systémů vytvářených lidmi však vzniká jistá míra nebezpečí, která nemůže nikdy být eliminována úplně na nulovou hodnotu. Proto se snažíme toto riziko udržet na co nejnižší přijatelné úrovni, jeho neustálým monitorováním a snižováním. Pro přijatelnou úroveň bezpečnosti je zavedený pojem **ALARP**, který vychází z anglické fráze: As Low As Reasonably Practicable. Což se dá chápat jako snížení rizika na co nejnižší úroveň, jaká je možná. Pojem ALARP se dá vysvětlit pomocí následujícího obrázku. Jak je vidět, každé riziko se dá vypočítat a přiřadit do určité části diagramu pomocí postupů popsaných v dalších kapitolách. Základem je, že se diagram rozděluje na tři části – přijatelná, nepřijatelná a mezi tím snesitelná. V případě přijatelného rizika je vše v pořádku a nemusí se nic dále řešit, v případě nepřijatelného rizika, musí být zastaveny další činnosti a v případě snesitelného rizika musí být přijaty opatření, ale činnost nemusí být zastavena. [6]




*Obr. 1.: ALARP [6]*

Při posuzování bezpečnosti se také musí hledět na to, zda dochází k letecké nehodě nebo pouze k incidentu. Je mezi nimi totiž velký rozdíl. Při incidentu většinou nedochází k žádnému, nebo pouze k velice malému zranění nebo poškození majetku. Naopak při letecké nehodě dochází k většímu poškození majetku nebo většímu zranění, až smrti osob, nebo jejich kombinaci. Rozdíl mezi leteckou havárií a incidentem je značný, protože podle průzkumu z roku 1969 vychází jedna smrtelná nehoda na asi 600 incidentů. Proto s leteckými incidenty již provozovatel v běžném provozu počítá a je připraven, že nastanou.

Dle statistiky leteckých nehod za rok 2014, zveřejněné Aviation Safety Network (ASN), došlo, i přes katastrofy dvou letů Malaysia Airlines, k historicky nejnižšímu počtu fatálních leteckých nehod v zaznamenané historii bezpečnosti civilní letecké dopravy. Uvedená fakta a statistiky dokládají, že létání patří a bude patřit mezi nejbezpečnější druhy dopravy. Z cca 33 000 000 letů za rok připadá 1 fatální letecká nehoda na 4 125 000 letů.

# 3 DOKUMENTY ZABÝVAJÍCÍ SE SMS

Hlavním dokumentem zabývajícím se v letectví programu řízení bezpečnosti je v této době ICAO Safety Management Manual Doc 9859, Third edition. Již třetí vydání tohoto dokumentu z roku 2013 plně nahrazuje jeho předchozí dvě vydání. Tento dokument Doc. 9859 by se spíše dal nazvat manuálem než předpisem. Jeho výsledkem má být vodítko pro členské státy, jak by systém řízení bezpečnosti měl vypadat. Jeho obsah se ovšem nezabývá jenom řízením bezpečnosti leteckých společností, ale také řízením bezpečnosti provozu letadel, způsobilosti letadel, letišť, řízení letového provozu a další související problematikou.

Kromě tohoto dokumentu se otázkou SMS zabývají i další dokumenty. Jedním z nich je Nařízení Komise (EU) č. 965/2012, které rozvádí a upřesňuje technické požadavky, které se týkají letového provozu podle nařízení Evropského parlamentu a Rady (ES) č. 216/2008. Toto nařízení v obchodní letecké dopravě stanovuje pravidla a povinnosti pro provoz letounů a vrtulníků. Dále se také zabývá i prohlídkami na odbavovací ploše pro letadla přistávající na letišti státu užívající tento dokument.

Mezi další dokumenty, jež se také zabývají systémem řízení bezpečnosti, určitě patří i Nařízení Komise EU č. 290/2012. V tomto nařízení je o řízení bezpečnosti napsáno v části Part-ORA, přesněji především v požadavku ORO.GEN.200 Systém řízení. Také k tomuto požadavku je vypracovaný poradní materiál, který jej specifikuje a rozvádí jednotlivé požadavky do větší hloubky a vyšel jako Směrnice CAA-FOD-01/2013.

Další dokumenty, ve kterých se řeší otázka řízení bezpečnosti, jsou přílohy (Annexy) vytvořené ICAO k Úmluvě. U nás v ČR jsou vydávány jako národní předpisy řady L, které jsou vydávány podle minimálních požadavků Annexů, doplněné o národní požadavky. Řízení bezpečnosti je popsáno především v těchto Annexech:

- Annex 6 – Provoz letadel
- Annex 11 – Letové provozní služby
- Annex 14 – Letiště
- Annex 19 – Řízení bezpečnosti

Poslední ze zmíněného seznamu, Annex 19, je z nich nejnovější. Byl vytvořen v roce 2012 a spolu s jeho zavedením vznikly i úpravy v některých starších annexech a tím byly doplněny o požadavky na systém řízení bezpečnosti.

Neméně důležité jsou v oblasti řízení bezpečnosti kromě těchto předpisů jejich vysvětlení a doplnění v dokumentech Přijatelné způsoby průkazu (AMC) a poradenský materiál (GM). Ty jak je již napsáno výše, doplňují jednotlivé části předpisů a podrobně popisují jejich jednotlivé části.

Na téma Řízení bezpečnosti již bylo napsáno několik diplomových prací se zaměřením na různé předpisy. Přehled několika takových prací, ze kterých je z části také čerpáno pro tuhle práci, je zde:

- ŠALANDA, M. *Zavedení systému řízení bezpečnosti u malého leteckého dopravce*. Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2008. 58 s. Vedoucí diplomové práce Ing. Ondřej Schaumann.
- MOKOŠ, M. *Vliv připravovaného ICAO Annex 19 na letecké provozovatele v ČR*. Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2013. 61 s. Vedoucí diplomové práce Ing. Jiří Chlebek, Ph.D.

# 4 VÝVOJ BEZPEČNOSTI V LETECTVÍ

Na konci roku 1903 poprvé vzlétli do vzduchu se svým letadlem bratři Wrightové. Již od této doby se muselo začít uvažovat nad bezpečností při létání. Jako první aspekt, na který se hledělo, byla technická stránka letadla. Podle toho se také nazývá toto první období jako technické období. Do současnosti se z hlediska vývoje bezpečnosti uvažují tři základní období:

## 4.1 Technické období

Toto období začínalo již na počátku dvacátého století a trvalo až do pozdních šedesátých let.

Na počátku tohoto období byla letecká technika v raném stádiu a s postupným vývojem a zaváděním nových a později i větších strojů docházelo k častějším leteckým nehodám. Tyto nehody vznikaly z počátku hlavně kvůli nedokonalému technickému stavu letecké techniky. Snaha o zvýšení bezpečnosti se tudíž zaměřovala na sledování a vyšetřování technických faktorů. Tímto krokem se v padesátých letech minulého století zvýšila bezpečnost létání a konstrukce letounů se držely podmínek daných technickými normami.

## 4.2 Období lidského faktoru

Období trvající od sedmdesátých let do poloviny devadesátých let minulého století.

V letecké dopravě je vliv lidského činitele velice důležitý parametr. Říká se, že chybovat je lidské a v letectví to platí opravdu ve značné míře, protože díky snížení počtu leteckých nehod v předchozím období v důsledku zpřísnění požadavků na technickou stránku letadel se letecká doprava stala o dost bezpečnější. Stále však docházelo ke značnému počtu nehod. Z vyšetřování těchto nehod vyplývalo, že ve značné míře mohl za nehody lidský činitel, včetně propojení člověk – stroj. Na počátku se hledělo na člověka výhradně jako na jednotlivce, bez propojení vztahů mezi jednotlivými členy posádky či celé organizace. Na propojení těchto vztahů a nehledění na posádku jako na jednotlivce, který pracuje ve složitém prostředí, se začalo hledět až na počátku devadesátých let minulého století. V této době se začalo uvažovat, že do pojmu lidský činitel spadají všichni lidé podílející se na životě letadla. Počínaje od návrhářů letadel, jejich konstruktérů, leteckých mechaniků, přes všechny techniky a obsluhu na letištích, piloty a v neposlední řadě všech lidí podílejících se na provedení a přípravě letů. Podle statistických údajů z vyšetřování leteckých nehod a incidentů vyplývá, že za 70% všech těchto nehod může právě lidský činitel. Pro pochopení, jak je do vztahů

v letectví zapojen lidský činitel se používá několik modelů, které jsou zaměřené na různé věci. Nejčastěji používané modely jsou model SHELL a „Reasonův model“.

### 4.2.1 Model SHELL

Tento model je sestaven na základě jednotlivých komponent, které působí na lidského činitele. Je složen, jak je vidět na obrázku, tak, že na člověka působí jednotlivé prvky. Poprvé byl použit roku 1972 profesorem Edwardem a později upraven roku 1975 prof. Hawkinsem.


*Obr. 2.: SHELL [3]*

Jednotlivá písmena v modelu SHELL znamenají:

- S … Software (postupy, symboly, atd.)
- H … Hardware (stroj)
- E … Environment (prostředí, ve kterém se odehrává interakce S – H – L)
- L … Liveware (člověk, jedinec v centru zájmu)
- L … Liveware (lidé, se kterými je jedinec v centru zájmu v nějakém vztahu) [3]

V tomto modelu se neřeší interakce, ve kterých nevystupuje člověk jedinec, tedy nezabývá se propojením například S-H, S-E apod.

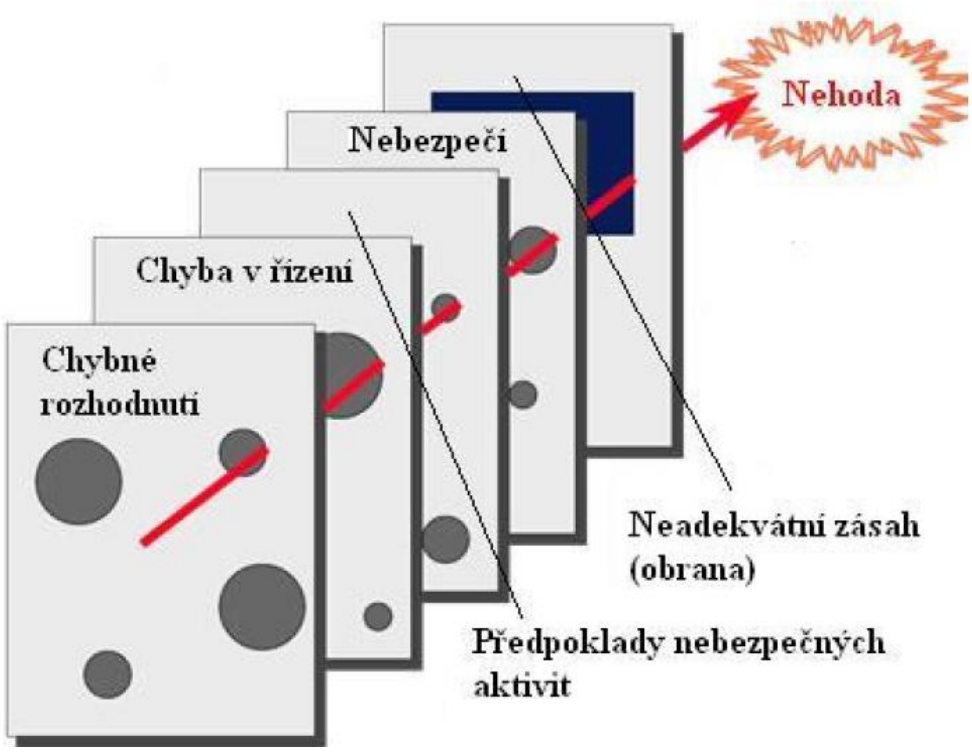
Uprostřed celého modelu je člověk, jedinec. Ten je nejkritičtější a zároveň nejflexibilnější část celého systému. Jsou na něj kladeny nejvyšší požadavky. Je vidět, že na obrázku nejsou styčné hrany hladké, což představuje, že vztahy mezi jednotlivými částmi nejsou pevné ani jednoduché. Tomuto propojení je potřeba věnovat velký význam, aby práce nevedla k selhání

nebo ke stresu jedince. Jelikož člověk je v centru modelu, ostatní části se musí adaptovat tak, aby společná práce byla co nejefektivnější. [3]

### 4.2.2 Reasonův model

Často také nazýván model švýcarského sýru. Jednotlivé plátky znázorňují různé úrovně organizace, jako je nejvyšší management, bezpečnostní systém, řadoví pracovníci, piloti a další. Otvory v jednotlivých vrstvách znamenají chyby v dané úrovni. Jestliže se chyby jednotlivých vrstev překrývají tak, že jimi prochází přímka, znamená to, že dojde k nehodě. Pomocí této metody lze najít chyby v celé organizaci napříč všemi úrovněmi a určit závažnost chyby, zda se jedná o hlavní, bezprostřední, či vedlejší.

Jednotlivé úrovně tohoto modelu se mohou kdykoli přidávat nebo odebírat, čímž se stává velice flexibilním. Díky jeho výhodám se používá jako základní metoda pro odhalování příčin leteckých nehod Americkým leteckým úřadem. [5]

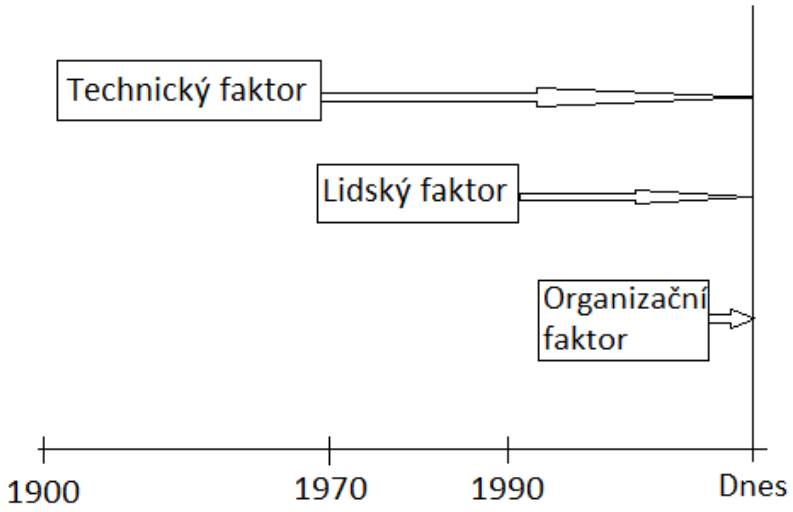



*Obr. 3.: Reasonův model [4]*

## 4.3 Období organizační

Zatím poslední období, které trvá od poloviny devadesátých let minulého století až do dnešní doby.

Bezpečnost v letecké dopravě začala být chápána z dalšího hlediska. Mimo technického činitele a lidského faktoru se zaměřuje na organizačního činitele. Vliv kultury a politiky řízení přináší nový pojem, jímž je „organizační nehoda“, což je vliv organizace na řízení a kontrolu bezpečnostního rizika. Dále již známý re-aktivní sběr údajů leteckých nehod a incidentů a jejich vyhodnocování byl doplněn o nový pro-aktivní přístup k bezpečnosti. Tento nový přístup je zaměřen na nepřetržitý sběr a analýzu dat, při kterém se využívá jak re-aktivní, tak pro-aktivní metody sledování bezpečnostních rizik a vyhledávání nově vznikajících problémů v otázce bezpečnosti. [2, 10]




*Obr. 4:* Vývoj bezpečnosti *[2,10]*

# 5 BEZPEČNOSTNÍ KULTURA ORGANIZACE PROVOZOVATELE

Jedním z nejdůležitějších faktorů správného fungování SMS je úroveň bezpečnostní kultury organizace. Pozitivní bezpečnostní kultura organizace musí být vytvářena „od shora dolů“. Úroveň bezpečnostní kultury je postavena na vzájemné důvěře mezi zaměstnavatelem a jednotlivými zaměstnanci, kteří musí mít jistotu, že hlášení bezpečnosti budou použita pro účel, který mají. Hlášení bezpečnosti nemají sloužit jako podnět pro postihy, ale pouze jako prevence před nebezpečím, avšak zaměstnanci toho nesmí využívat a musí si uvědomit, že nedbalost nebo hrubé porušení pravidel nemůže být tolerováno.

Kvalita bezpečnostní kultury v důsledku závisí na chování všech jednotlivců i skupin v organizaci. Závisí na takovém jejich chování, jenž průběžně zvyšuje nebo alespoň udržuje úroveň bezpečnosti. Dále závisí na jejich vůli přizpůsobit se a postavit se problémům bezpečnosti a na vyhodnocování reakcí týkajících se problémů bezpečnosti.

Je potřeba si uvědomit, že základem správného fungování zabezpečení bezpečnosti je spolehlivý systém ohlašování incidentů/nehod. Hlášení nedostatku v oblasti bezpečnosti by se měli účastnit všichni zaměstnanci organizace a měl by fungovat systémem, pokud máš nějakou pochybnost z hlediska bezpečnosti, ohlas to. Všechna získaná hlášení musí být dále řádně prošetřena a vytvořena pravidla pro jejich prevenci.

Aby bezpečnostní systém společnosti byl účinný, musí se na jeho vytváření podílet všichni, začínaje vrcholovým vedením. Musí být kladen velký důraz na zjištění všech příčin pochybení a vykonány kroky k jejich potlačení. Zaměstnanci musí mít důvěru v systém a popřípadě být za hlášení odměňováni. [2, 10]

Organizace můžeme rozdělit na tři kategorie podle toho, jak se stavějí k informacím o nebezpečí ve společnosti a k jeho řízení. Rozdělení je uvedeno v následující tabulce:

| Bezpečnostní kultura / Charakteristiky | Špatná | Byrokratická | **Pozitivní** |
|---|---|---|---|
| Oznámení je: | Potlačeno | Ignorováno | **Vyhledáváno** |
| Zaměstnanci, kteří nebezpečí oznámí, jsou: | Odrazováni | Trpěni | **Povzbuzováni, odměňováni** |
| Odpovědnost za bezpečnost je: | Vyhýbavá | Roztříštěná | **Sdílená** |
| Šíření bezpečnostních informací je: | Odrazováno | Dovoleno, ale odrazováno | **Zajištěno a odměňováno** |
| Selhání vede k: | Přikrytí | Lokálnímu zafixování | **Šetření a nápravě** |
| Nové nápady jsou: | Potlačovány | Považovány za nový problém | **Vítány a podporovány** |

*Tab. 1.: Druhy bezpečnostní kultury [2]*

Nezáleží na velikosti, složitosti ani typu organizace, protože aby systém řízení bezpečnosti úspěšně fungoval, záleží na tom, kolik času, pozornosti a prostředků věnuje vrcholové vedení do jeho řízení.

Výslednou odpovědnost za přístup k bezpečnosti organizace má celé vedení organizace. *„Positivní bezpečnostní kultura organizace bude záviset na úrovni závazků, postoje a přístupu vrcholového vedení k zajištění bezpečného provozu.“ [2]*

# 6 STRUKTURA IMPLEMENTACE SMS

V této kapitole je popsána struktura implementace SMS provozovateli obchodní letecké dopravy. Je také potřeba si uvědomit, že rozsáhlost této struktury musí odpovídat velikosti organizace, organizaci jejího provozu a jeho složitosti.

Každá struktura implementace SMS musí zahrnovat minimálně čtyři komponenty. Ty jsou následující:

1. Politika a záměry/cíle bezpečnosti
2. Řízení bezpečnostního rizika
3. Ověřování úrovně bezpečnosti
4. Podpora bezpečnosti

Tyto čtyři komponenty dále obsahují několik prvků daných ICAO SMS strukturou popsaných níže, podle

- zdroje č. 2: VLČEK, F. Směrnice CAA-FOD-01/2013: Poradní materiál k požadavku ORO.GEN.200 systém řízení. 2013. a
- zdroje č. 10: ICAO: Safety Management Manual (SMM). Doc. 9859, Montreal, 2006

## 6.1 Politika a záměry/cíle bezpečnosti

### 6.1.1 Závazek a odpovědnost vedení

Úkolem provozovatele je definovat bezpečnostní politiku organizace tak, aby byla v souladu s mezinárodními i národními předpisy a odpovědný vedoucí to musí potvrdit svým podpisem. Součástí politiky bezpečnosti musí být závazek organizace, že budou zajišťovány a hlavně poskytovány maximální zdroje týkající se bezpečnosti a umožňující vytvářet pozitivní politiku bezpečnosti. Do systému hlášení a řízení bezpečnosti se musí zapojovat všichni členové organizace, počínaje vrcholovým vedením. Dalším bodem by měly být postupy, jak realizovat hlášení týkající se bezpečnosti. Musí být charakterizováno, jaké typy chování jsou nepřijatelné a za jakých podmínek by se nemělo přistupovat k disciplinárním opatřením. Veškeré body musí být neustále kontrolovány, aby se zajistilo, zda daná politika je nastavena a udržována v patřičném stavu k dané organizaci.

### 6.1.2 Odpovědnosti za bezpečnost

Úkolem provozovatele je určit odpovědného vedoucího, který je zodpovědný za celý SMS. Jeho práce spočívá v zavádění a udržování SMS. Dále musí provozovatel stanovit odpovědnosti všech členů vrcholového vedení a samozřejmě také všech dalších pracovníků. Pravomoci a odpovědnosti jednotlivých členů musí být známy a sdělovány všem napříč celou organizací a také musí být vymezena úroveň řízení s pravomocí přijímat rozhodnutí o snesitelnosti/přípustnosti bezpečnostního rizika. Provozovatel je mimo jiné odpovědný také za bezpečnost všech produktů a služeb, jenž na základě smluv přijímá od externích dodavatelů.

### 6.1.3 Jmenování klíčového personálu ve vztahu k bezpečnosti

Povinností provozovatele je jmenování vedoucího bezpečnosti, jenž je odpovědnou osobou za koordinaci při implementaci a udržování SMS na patřičné úrovni.

Ve složitých organizacích by měl být zřízen kromě funkce vedoucího bezpečnosti navíc také Výbor pro přezkoumávání bezpečnosti. Členy výboru pro přezkoumávání bezpečnosti by měli být jednotliví vedoucí pracovníci všech funkčních oblastí, přičemž vedoucí bezpečnosti také smí byt jeho členem. Další formou může také být Akční skupina pro bezpečnost, ta může být zřízena buď trvale nebo jako Ad-Hoc skupina, jenž vypomáhá nebo jedná jménem Výboru pro přezkoumávání bezpečnosti.

V nesložitých organizacích postačuje funkce vedoucího bezpečnosti, avšak v případě potřeby by mu měli být nápomocni další členové organizace provozovatele pro rychlejší vyřešeni dané situace.

### 6.1.4 Koordinace plánu reakce na nouzové situace

Povinností provozovatele je zajistit plán reakce na nouzové situace (Emergency Response Plan-ERP), jenž poskytuje plynulý a bezpečný přechod z normálního na nouzový režim a opět zpět na normální provoz. Provozovatel musí taktéž zajistit koordinaci s plány reakce s organizacemi, se kterými je provozovatel propojen při poskytování svých služeb. Velikost a rozsah ERP je závislý na velikosti, povaze a složitosti činností vykonávajících organizací provozovatele a měl by být popsán v samostatném dokumentu.

### 6.1.5 SMS dokumentace

Povinností provozovatele je vytvořit a udržovat dokumentaci SMS, jenž musí obsahovat politiku a úkoly bezpečnosti, požadavky SMS, procesy a postupy SMS, pravomoci a odpovědnosti za procesy a postupy a výstupy SMS. Dále musí provozovatel vytvořit

a udržovat příručku řízení bezpečnosti (Safety Management Manual-SMM), aby bylo zajištěno sdílení a šíření přístupu k řízení bezpečnosti napříč celou organizací provozovatele.

Příručka řízení bezpečnosti (SMM) má být hlavním dokumentem organizace provozovatele pro sdělování přístupu k bezpečnosti. V této příručce mají být popsány všechny zřetele řízení bezpečnosti, bezpečnostní politika, cíle, postupy a odpovědnosti jednotlivých členů organizace za bezpečnost. SMM nesložitého provozovatele musí obsahovat všechny tyto položky, ale postačuje ve zjednodušené formě s ohledem na velikost, povahu a složitost organizace.

SMM může být vypracován jako samostatný dokument, nebo může byt zakomponován do jedné nebo více příruček, s tím, že jednotlivé části příruček musí na sebe odkazovat.

## 6.2 Řízení bezpečnostního rizika

Řízení bezpečnosti je systematické řízení rizik spojených s letovým provozem, související s pozemními operacemi letadel, inženýrskými činnostmi nebo činnostmi údržby, k dosažení vysoké úrovně bezpečnostních výkonů.

Řízení rizika ve společnosti můžeme všeobecně rozdělit na tři části:

- **Proces zjišťování/identifikace nebezpečí** – je zajištěn dvěma formami, re-aktivním a pro-aktivním programem, což jsou prostředky pro sběr, zaznamenávání, analýzu, reakci a vytváření zpětné vazby týkající se nebezpečí a s nimi spojených rizik, jenž ovlivňují bezpečnost provozních činností provozovatele. Všechny systémy hlášení musí mít zajištěn proces zpětné vazby.

- **Proces vyhodnocení a zmírnění rizika** – organizace by měly mít zavedený proces řízení rizik, zajišťující analýzu, vyhodnocení a kontroly rizik na minimální hodnotu.

- **Interní bezpečnostní vyšetřování** – mělo by zahrnovat nejen ty události, jež je potřeba hlásit na daném úřadu a řešit tak i ty nejmenší události.

Proces vyhodnocování rizika začíná zjištěním nebezpečí, jež je nepříznivé pro provoz, následuje vyhodnocení pravděpodobnosti jeho vzniku a jeho závažnosti. Když je zjištěna úroveň rizika, jsou podniknuty kroky pro jeho snížení na minimální hodnotu. Tyto předchozí kroky jsou neustále opakovány a kontrolovány, jestli je snížení rizika dostačující.

Řízení bezpečnostního rizika v nesložitých organizacích se smí provádět ve zjednodušené formě, a to například za pomocí kontrolních seznamů nebezpečí (hazard checklist) nebo podobných nástrojů pro řízení rizika nebo procesů.

### 6.2.1 Zjišťování/identifikace nebezpečí

Povinností provozovatele je zavézt proces identifikace nebezpečí ohrožujícího provoz. Tento proces má být vytvořen na kombinaci reaktivního, pro-aktivního a pre-dektivního řízení sběru informací.

**Nebezpečí** – obecně je to existující stav, okolnost nebo předmět, díky kterému může vzniknout poranění nebo smrt osob, poškození, zničení nebo ztráta schopnosti pro vykonání požadovaného výkonu.

**Riziko neboli následek** – je nebezpečí, které by mohlo pravděpodobně nastat.

Předpokladem pro spolehlivé řízení bezpečnostního rizika a jeho předcházení je neustálé monitorování a identifikace nebezpečí.

Důvodů vzniku nebezpečí mohou být rozděleny na přírodní, technické, ekonomické, ergonomické nebo organizační. Z těchto nebo jiných důvodů může nebezpečí vznikat nejčastěji v organizaci provozovatele nebo v organizaci údržby letadel.

*Metody a zdroje zjišťování / identifikace nebezpečí*

Zjišťování nebezpečí je nekončící proces, který stále pokračuje. Identifikovat nebezpečí a s ním spojená rizika lze pouze tehdy, když víme o jeho existenci. Pro zjištění skrytých problémů a stavů, jež by mohly ohrozit bezpečnost, musí v organizacích fungovat systémy povinných bezpečnostních hlášení.

Důležité je si uvědomit, že systém hlášení nebezpečí v organizaci má sloužit pouze jako prevence, nikoli jako zdroj pro posuzování viny v případě, kdy došlo k omylu. Z tohoto důvodu je potřeba usilovat o vytvoření takové atmosféry, aby se nikdo nebál následků a aby všichni otevřeně a bez strachu vše hlásili. Pro co nejpřesnější zhodnocení daného nebezpečí a předcházení mu je důležité zajistit zpětnou vazbu k tomu, kdo incident hlásil.

#### *6.2.1.1 Metody zjišťování / identifikace nebezpečí*

Zjišťování nebezpečí v organizaci začíná definováním strategie pro prevenci nehod. Strategie bude odrážet firemní kulturu bezpečnosti a může se pohybovat v rozmezí od čistě re-aktivní, jenž reaguje pouze na nehody, přes strategie, které jsou velmi aktivní při hledání

bezpečnostních problémů. V závislosti na přijaté strategii pro prevenci nehod je potřeba použít různé metody a nástroje.

**Re-aktivní strategie**

Re-aktivním přístupem je označena taková metoda řízení bezpečnosti, kdy se vychází z poznatků z vyšetřování leteckých nehod a incidentů, které se již v minulosti staly. Pomocí předchozích nehod se zjišťují chyby, jenž provedl někdo dříve. Těmto chybám se lze v budoucnu vyvarovat, například úpravou postupů.

**Pro-aktivní strategie**

Pro-aktivní přístup znamená, že se na řízení bezpečnosti díváme v reálném čase. Sledujeme vlastní reálný provoz, reálné děje a dění ve společnosti a na tom zakládáme řízení bezpečnosti. Pro tuto metodu využíváme vnitřní audity společnosti, dále hlášení nebezpečí od zaměstnanců a ihned je vyhodnocujeme pro zabránění jakékoli nehody v aktuálním provozu.

**Prediktivní strategie**

Metoda prediktivní je založena na vyhledávání chyb systému se zaměřením na budoucí události. V této metodě je důležitý sběr dat a systémových procesů z celého provozu organizace a jejich analýza a vyhodnocování. Jakékoli zjištěné nedostatky ohrožení bezpečnosti vedou k činnosti pro jejich odstranění nebo alespoň zmírnění do budoucna.

Ve vyspělých systémech řízení bezpečnosti se využívá kombinací předešlých strategií. Jestliže však organizace nevyužívají kombinací všech, je výhodné použít strategie pro-aktivní nebo prediktivní. Tyto dvě strategie totiž nespoléhají na řízení podle předchozích událostí, ale zkoumají aktuální a budoucí dění.

#### *6.2.1.2 Zdroje zjišťování / identifikace nebezpečí*

Zdroje využívané pro identifikaci nebezpečí organizace můžeme rozdělit na dvě skupiny:

**Interní**

Zde spadá především hlášení nebezpečí v organizaci, dále hlášení za letu, interní vyšetřování, analýza provozních letových údajů, záznamy z výcviků, monitorování letových posádek, údaje z minulých nehod a incidentů a další.

**Externí**

Z externích zdrojů to jsou záznamy nehod jiných provozovatelů, závěrečné zprávy vyšetřování leteckých nehod a incidentů, zprávy z auditů provedených UCL, EASA, apod., nálezy SAFA

(Safety Assessment of Foreign Aircraft) / SACA (Safety Assessment of Community Aircraft), zprávy z IOSA auditů (IATA Operations Safety Audit).

### 6.2.2 Vyhodnocení a zmírnění rizika

Povinností provozovatele je zajistit zavedení a udržování procesu, jenž zajistí analýzu, kontrolu a vyhodnocení bezpečnostního rizika v provozu.

#### *6.2.2.1 Proces vyhodnocení rizika*

Hlavním důvodem, proč se vyhodnocuje riziko nebezpečí, je zjistit, jaký je jeho potenciál způsobit škodu. Proto by se mělo riziko vyhodnocovat ze dvou hledisek, vážnosti a pravděpodobnosti následků. Po zjištění úrovně rizika by měla následovat eliminace rizika nebo alespoň jeho snížení na co nejnižší možnou úroveň (ALARP). Toto snížení může být realizováno buď snížením pravděpodobností nastoupení rizika, nebo snížením vážnosti jeho následků.

V následujících tabulkách je zobrazeno, na co je potřeba se zaměřit při klasifikaci rizika. První tabulka nám udává hodnotu pravděpodobnosti nastoupení daného rizika, čím vyšší hodnota, tím vyšší pravděpodobnost nastoupení. Ve druhé tabulce je každému riziku přiřazen význam neboli dopad, jaký riziko s sebou přináší. Ukazuje, zdali je zanedbatelné nebo vede ke katastrofě. Za těmito tabulkami je další tabulka, matice vyhodnocení rizika, která slučuje předchozí a dává nám jasnou představu, zda je riziko přijatelné, snesitelné nebo nepřijatelné. Podle matice vyhodnocení rizika je potřeba dále se rozhodovat, jak s rizikem nakládat, zda jej ponechat nebo vykonat kroky pro jeho eliminaci.

| Možná pravděpodobnost | Význam | Hodnota |
|---|---|---|
| Častá | Pravděpodobnost, že se může stát velmi často | 5 |
| Občasná | Pravděpodobnost, že se může někdy stát | 4 |
| Časově vzdálená | Nepravděpodobné, ale s možností, že se může stát | 3 |
| Nepravděpodobná | Velmi nepravděpodobné, že by se mohlo stát | 2 |
| Extrémně nepravděpodobná | Téměř nemyslitelné, že by se takový případ mohl stát | 1 |

*Tab. 2.: Klasifikace možné pravděpodobnosti rizika [2]*

| Vážnost | Význam | Hodnota |
|---|---|---|
| Katastrofická<br>Catastrophic | Výsledkem je nehoda, úmrtí a/nebo zničení zařízení | A |
| Nebezpečná<br>Hazardous | Rozsáhlé snížení míry bezpečnosti, vážné zranění nebo závažné poškození zařízení | B |
| Závažná<br>Major | Významné snížení míry bezpečnosti, vážný incident nebo zranění osob | C |
| Méně závažná<br>Minor | Použití nouzových postupů, méně závažný incident | D |
| Zanedbatelná<br>Negligible | Malé následky | E |

*Tab. 3.: Klasifikace vážnosti rizika [2]*

| Pravděpodobnost rizika | Vážnost rizika | | | | |
|---|---|---|---|---|---|
| | Katastrofická<br>Catastrophic | Nebezpečná<br>Hazardous | Závažná<br>Major | Méně závažná<br>Minor | Zanedbatelná<br>Negligible |
| Častá | **5A** | **5B** | **5C** | **5D** | **5E** |
| Občasná | **4A** | **4B** | **4C** | **4D** | **4E** |
| Časově vzdálená | **3A** | **3B** | **3C** | **3D** | **3E** |
| Nepravděpodobná | **2A** | **2B** | **2C** | **2D** | **2E** |
| Extrémně nepravděpodobná | **1A** | **1B** | **1C** | **1D** | **1E** |

*Tab. 4.: Matice vyhodnocení rizika [2]*

Nepřijatelné – vysoké riziko: v tomto případě musí být provoz neodkladně přerušen a riziko musí být eliminováno.

Snesitelné – přiměřené riziko: riziko je snesitelné, ale je neustále snaha o jeho snížení

Přijatelné – nízké riziko: riziko je tak nízké, že je možné pokračovat bez omezení, ale riziko musí být nadále kontrolováno a musí se mu stále věnovat vysoká pozornost.

#### *6.2.2.2 Zmírnění bezpečnostního rizika/ kontrola*

Jsou postupy pro odstranění možného bezpečnostního rizika, velikosti jeho následků nebo velikosti pravděpodobnosti jeho nastoupení. Ke snížení rizika se používají obranná opatření, jež jsou specifické kroky zavedením preventivních opatření pro zabránění nebezpečným situacím.

Používá se více druhů obranných opatření. Některá z nich jsou technická – zavedení nového zařízení nebo struktury, dále výcviky, pravidla, postupy a standartní provozní postupy (SOP) a samozřejmě spoustu dalších postupů pro snížení/zrušení možného rizika. Na snížení rizika lze použít i několik strategií, mezi nejpoužívanější však patří varování (je zrušený provoz, čímž se odstraní riziko), omezení (četnost provozu nebo činností se omezí pro omezení vážnosti rizika) a izolace (podniknuty kroky pro izolování účinků následku rizika).

#### *6.2.2.3 Záznam o nebezpečích*

Záznamy o nebezpečích se musí vyhotovovat pro všechna zjištěná nebezpečí, jejich vyhodnocení a všechny další kroky. Výborným systémem pro jejich záznam je např. použití Záznamu o nebezpečích a vyhodnocení bezpečnostního rizika. Tyto záznamy musí vždy obsahovat: zjištěné nebezpečí a související rizika, dále výsledky vyhodnocení rizik spolu se stávajícími opatřeními i následujícími opatřeními pro zmírnění rizik a na závěr ještě opětovné zhodnocení rizik, díky kterému se porovná, zda došlo ke zlepšení. Záznamy o nebezpečích jsou důležitou součástí registru bezpečnostních údajů SMS.

## 6.3 Ověřování úrovně bezpečnosti

Bezpečnostní kritéria, jenž jsou založena na datech využívaných pro sledování a vyhodnocování výkonnosti v bezpečnosti, jsou ukazatele výkonnosti v bezpečnosti. Provozovatelé mají stanoveny ukazatele a cíle výkonnosti v bezpečnosti a tyto dosahované výsledky se nazývají Výkonnost v bezpečnosti. Ověřování úrovně bezpečnosti je tedy vše, co provozovatel dělá pro sledování a hlavně ověřování výkonnosti v bezpečnosti. Tímto procesem si provozovatel ověřuje výkonnost celého SMS, ověřuje, že proces zjišťování nebezpečí a proces zmírnění rizik funguje efektivně a jsou realizována přiměřená opatření.

### 6.3.1 Sledování, hodnocení a průběžné zdokonalování výkonnosti v bezpečnosti

Povinností provozovatele je ve své organizaci vytvořit a udržovat prostředky pro sledování stavu bezpečnosti a neustále prokazovat účinnost řízeni rizik bezpečnosti. Organizace musí především ověřovat výkonnost v bezpečnosti s důrazem na ukazatele výkonnosti v bezpečnosti (SPI) a cíle výkonnosti v bezpečnosti SMS. Další podmínkou je také průběžné zvyšování výkonnosti v bezpečnosti, spolu s vylepšováním celého SMS.

Podmínkou řízení výkonnosti organizace je stanovit míru výkonnosti a bezpečnostní data. Pro toto je důležité stanovit v organizaci ukazatele výkonnosti v bezpečnosti (SPI). Každá organizace si může stanovit jiné ukazatele výkonnosti v bezpečnosti v závislosti na své organizaci. Mezi nejčastěji používané SPI patří počet incidentů, vážných incidentů, hlášení, dobrovolných hlášení, stížností zákazníků, provedených průzkumů, zaměstnanců proškolených na SMS, a mnoho dalších. Stanovení ukazatelů SPI by se neobešlo bez cílů výkonnosti v bezpečnosti. Cíle výkonnosti v bezpečnosti se stanovují, aby se mohla porovnávat výkonnost. Nejčastějším příkladem cílů výkonnosti v bezpečnosti je např.: snížit počet incidentů na…, snížit počet vážných incidentů o…, zvýšit počet hlášení na…, apod. Tyto údaje by se pravidelně měly kontrolovat a přezkoumávat.

Sledování a hodnocení výkonnosti v bezpečnosti organizace má být proces, během něhož se ověřuje aktuální úroveň výkonnosti v bezpečnosti se záměry a cíli bezpečnosti. Činnost sledování a hodnocení by se měla skládat z těchto bodů:

- Bezpečnostní hlášení – zabývající se stavem dodržování daných požadavků
- Bezpečnostní studie – zahrnující širší spektrum bezpečnostních problémů
- Bezpečnostní posuzování – také posouzení tendencí, souvisejících se zaváděním nových technologií, či postupů, do praxe
- Bezpečnostní audity – zaměřené na integritu SMS a vyhodnocování bezpečnostního rizika v pravidelných intervalech
- Bezpečnostní průzkumy dotazováním – zaměřené na prověření jistých prvků či postupů názory provozního personálu

Průběžné zdokonalování výkonnosti v bezpečnosti by měl provozovatel dosahovat nejlépe proaktivním a reaktivním hodnocením vybavení, dokumentace a postupů, bezpečnostními audity a průzkumy. Proaktivním hodnocením jednotlivců, se zaměřením na plnění svých povinností. A dále reaktivním hodnocením účinnosti systému kontroly a zmírnění rizika.

Úlohou vedoucího bezpečnosti a vedoucího sledování shody je vyhotovit minimálně jednou ročně zprávu pro odpovědného vedoucího o stavu, jak spolehlivě je bezpečnost řízena a o tom, jak efektivně SMS pracuje, společně s návrhem pro zdokonalení. Důležitým bodem zprávy by mělo být srovnání s úrovní předešlého roku.

### 6.3.2 Řízení změn

Mezi další povinnosti provozovatele organizace patří vytvořit a udržovat systém identifikace změn. Identifikovat a prověřovat každou změnu je důležité z hlediska udržení jisté kvality služeb, tak aby nedošlo zavedením nové služby nebo procesu ke zhoršení jejich kvality. Tento systém musí obsahovat postup, co musí být vykonáno před tím, než bude jakákoli změna implementována. Pro proces zavádění jakékoli změny může být použit již aktuální proces provozovatele pro zjišťování / identifikaci nebezpečí, vyhodnocování a zmírňování rizika. Proces řízení musí samozřejmě být zdokumentován. Výbornou cestou pro dokumentaci změn je zavedení změnového formuláře, jenž zahrnuje všechny body pro vyhodnocení dopadu změny.

## 6.4 Podpora bezpečnosti

Nejdůležitějšími členy v bezpečnosti organizace jsou manažeři, protože právě oni jdou příkladem všem ostatním. To znamená, že pokud se manažeři neangažují v otázkách bezpečnosti, pak ani ostatní zaměstnanci nejsou nuceni k dodržování bezpečnosti. Pro podporu a prosazování bezpečnosti se využívá hlavně dvou důležitých procesů: bezpečnostního výcviku a bezpečnostní komunikace.

### 6.4.1 Bezpečnostní výcvik

Bezpečnostní výcvik je důležitým procesem při zvyšování bezpečnosti v celé organizaci a celém SMS provozovatele. Proto je povinností provozovatele vytvořit systém bezpečnostních výcviků zaměřený na všechny činnosti ve své organizaci. Absolvovat bezpečnostní výcviky jak během počátku práce v organizaci, tak především i v průběhu v pravidelných intervalech musí všichni zaměstnanci, počínaje vrcholovým vedením, přes vedoucí pracovníky až po provozní personál. Není však podmínkou, aby všichni zaměstnanci absolvovali všechny kurzy zaměřené na všechny činnosti. Postačuje, aby rozsah bezpečnostního výcviku byl přímo úměrný činnostem, které vykonávají ve své organizaci a se kterými přijdou do styku.

Provozovatel by měl také zavést pro každého svého pracovníka vlastní složku, ve které budou všechny údaje o něm a o všech školeních, které absolvoval. Kromě školení, které absolvoval,

by měla obsahovat i informace, kdy přesně a které školení absolvoval a v neposlední řadě také plán, kdy a jaké školení má opět absolvovat.

V následující tabulce je nástin některých SMS výcviků, které by měly být poskytnuty zaměstnancům:

| Obsah | Cíle výcviku |
|---|---|
| Politika bezpečnosti | Porozumět hlavním prvkům politiky bezpečnosti provozovatele. |
| Organizace, role a odpovědnosti | Porozumět organizaci, rolím a odpovědnostem, týkajících se SMS. Každý by měl znát svoji vlastní roli/funkci v SMS. |
| Bezpečnostní záměry/cíle | Porozumět záměrům/cílům, které hodlá provozovatel dosáhnout v bezpečnosti. |
| Plán reakce na nouzové situace (ERP), včetně pravidelného praktického nácviku | Porozumět různorodé škále rolí a odpovědností v ERP společnosti. |
| Každý by měl znát svoji vlastní roli/funkci v ERP. | Hlášení událostí a nebezpečí |
| Znát prostředky a postupy pro hlášení událostí a nebezpečí. | Proces řízení bezpečnostního, včetně rolí a odpovědností. |
| Porozumět procesu řízení bezpečnostního rizika. | Každý by měl znát svojí vlastní roli v procesu řízení bezpečnostního rizika. |
| Průběžné zdokonalování výkonnosti v bezpečnosti | Porozumět principům průběžného zdokonalování výkonnosti v bezpečnosti. |
| Sledování shody | Porozumět základním principům sledování shody. |
| Odpovědnosti při využívání externích dodavatelů | Porozumět odpovědnostem provozovatele při využívání služeb od externích dodavatelů. Každý by měl znát svoji vlastní roli a odpovědnosti, týkajících se této záležitosti… |

*Tab. 5.: Bezpečnostní SMS výcviky [2]*

Programy a druh jednotlivých školení mohou probíhat několika formami, které mohou být také kombinovány. Školení se mohou skládat z přednášek v učebnách provozovatele, ze samostudia pomocí učebních materiálů i ze sdělovacích prostředků, kterými jsou odborné články nebo odborné magazíny o bezpečnosti v civilním letectví. Dalšími formami mohou také být elearningové kurzy nebo kurzy poskytované jinou organizací zaměřující se na bezpečnost. Bezpečnostní výcviky mohou provádět v organizaci provozovatele samozřejmě členové dané organizace, avšak před tím musí sami absolvovat SMS výcvikový kurz ve schválené a oprávněné organizaci pod záštitou ICAO, EASA, JAA Training apod.

### 6.4.2 Bezpečnostní komunikace

Komunikace ve společnosti je velice důležitým faktorem pro řízení bezpečnosti. Provozovatel organizace by měl zajistit, aby veškerý personál byl obeznámen s aktuálním děním v organizaci v otázce bezpečnosti. Všichni by měli znát činnosti SMS, mělo by být zajištěno sdělování hlavních bezpečnostních informací a měly by být vysvětleny důvody, proč byly podniknuty dané kroky a přijatá daná opatření související s bezpečností.

Bezpečnostní komunikaci lze zajistit několika způsoby, jedním z nich mohou být bezpečnostní schůzky s personálem, vedené v přátelském duchu a otevřené diskuzi. Další možností je komunikace pomocí e-mailu, pomocí webových stránek provozovatele nebo vyvěšováním informací na nástěnky. V zásadě je však komunikace obousměrný proces, proto záleží na daném provozovateli, jakou metodu komunikace zvolí, či kombinaci více metod.

# 7 ROZBOR NABÍZENÝCH SOFTWAROVÝCH NÁSTROJŮ

Na internetu lze v dnešní době nalézt několik již vytvořených a připravených softwarových nástrojů pro podporu safety managementu v letectví. Jednotlivé nástroje nabízejí různé společnosti a většinou jsou ještě rozděleny na více úrovní, podle toho co nabízejí. V následující části jsou popsány některé softwarové nástroje, jež lze použít.

Všechny níže uvedené softwarové nástroje jsou produkty firem a jsou tedy placené. Jakou cenu za tyto produkty požadují jednotlivé firmy, je těžké říci. Jako ukázku lze považovat tabulka u produktu SMS Pro, kterou zveřejňuje společnost na svých webových stránkách. Ostatní společnosti cenu nezveřejňují a vypočítávají ji po osobní schůzce s vedením organizace podle specifických informací o společnosti. Některé z uvedených společností byly dotázány za účelem cenové nabídky, ale protože nešlo o skutečného potencionálního zákazníka, odmítly se vyjádřit. Kvůli tomuto nejsou u dalších produktů uvedeny ceny za softwarový nástroj.

## 7.1 SMS Pro

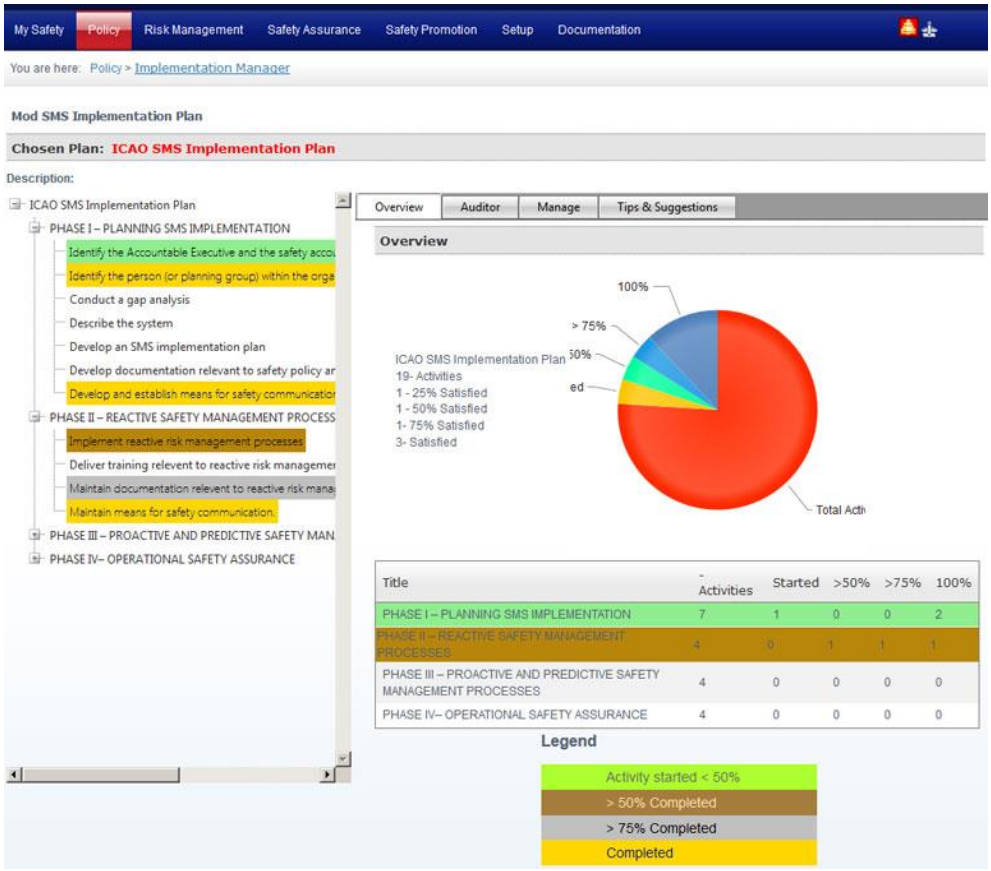
Program SMS Pro nabízí na trh společnost *NorthWest Data Solutions* (NWDS). Tato společnost vznikla v roce 2003 a je poskytovatelem informačních technologií a poradcem pro organizace všech velikostí. NWDS se svými aplikacemi zaměřují na široký okruh odvětví průmyslu. Specializují se však především na navrhování a vývoj webových aplikací, a to pro průmysl obrany, financí, letectví a strojírenský průmysl. Společnost NorthWest Data Solutions započala v roce 2005 s vývojem komerčního softwarového nástroje určeného speciálně pro letecký průmysl, na který kladla tyto požadavky:

- Uživatelsky přívětivý
- Na webové bázi
- Řešený podle požadavků ICAO
- Vhodný pro letiště, letecké společnosti, všeobecné letectví
- Přizpůsobitelný
- Cenově dostupný.

Systém SMS Pro je v provozu od počátku roku 2008 a je používán tisíci odborníky na celém světě. SMS Pro využívají především mezinárodní i místní letiště, letecké společnosti, provozovatelé vrtulníků a zdravotnická doprava. Struktura systému je vytvářena podle požadavku dokumentu Doc. 9859 ICAO, ale požadavky jsou uzpůsobeny tak, aby vyhovoval

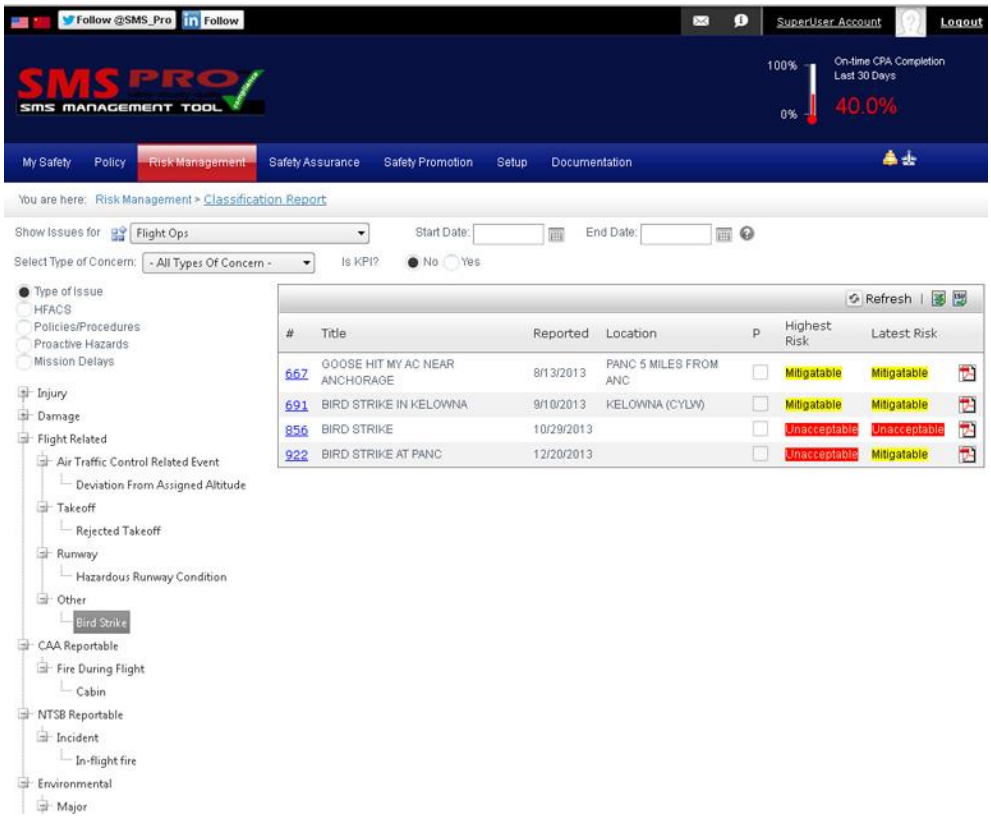
i dalším předpisům, jež vydávají organizace civilního letectví, jako jsou FAA, EASA a další. Působnost softwaru SMS Pro se zaměřuje na celou společnost a je postaven na následujících čtyřech pilířích: Průzkum bezpečnostní politiky, průzkum bezpečnosti řízení rizik, zajištění bezpečnosti a podpora bezpečnosti.

Kromě čtyř základních pilířů obsahuje hlavní menu softwaru další záložky nastavení. Mezi ně patří záložka obsahující základní informace o společnosti, nastavení programu, dokumenty organizace, jež jsou zde uloženy a jsou kdykoli hned po ruce. Mezi dokumenty mohou patřit veškeré příručky, checklisty, provozní postupy, postupy pro technické prohlídky a samozřejmě si zde provozovatel může nahrát jakékoli další dokumenty. V neposlední řadě se zde nachází odkaz i na politiku společnosti. Do politiky například spadá úroveň a postup implementace společnosti. Implementace systému řízení bezpečnosti se rozkládá, jak je napsáno výše v předchozí kapitole, do čtyř základních fází a každá fáze obsahuje několik bodů, které musí být vykonány. V softwaru SMS Pro jsou jednotlivé body plánu přichystány a podle barevného označení jednotlivých částí lze vidět, co je již hotovo a co je třeba ještě udělat nebo dodělat. Ukázka zobrazení implementace systému je naznačena na následujícím obrázku.




*Obr. 5.: SMS implementation plan [17]*

Nedílnou součástí systému řízení bezpečnosti je systém hlášení incidentů/nehod. Software SMS Pro má vytvořené formuláře, jenž se vyplňují pomocí nabídek možností. Díky této funkci se podané zprávy o událostech automaticky roztřídí do různých skupin, podle toho čeho se týkají. Toto rozdělení může být závislé např. na tom, při jaké fázi letu se událost stala nebo jaké části letadla se problém týká nebo dle závažnosti problému. Názorná ukázka, jak zobrazení vypadá v softwaru SMS Pro lze vidět na následujícím obrázku.




*Obr. 6.: Classification report [17]*

Společnost NorthWest Data Solutions nabízí svůj software SMS Pro ve čtyřech základních úrovních, rozdělených podle služeb, které nabízí:

Nejjednodušší verze s názvem STARTER. SMS Pro Starter nabízí neuvěřitelné úspory pro šetrné společnosti, které potřebují vysoce kvalitní software pro řízení bezpečnosti letecké dopravy, aniž by vznikly vysoké počáteční investice. Jeho cena začíná již na padesáti dolarech za měsíc pro organizace s jedním až dvaceti zaměstnanci, při větším počtu zaměstnanců cena stoupá.

Druhá verze, nazvaná BASIC, je ekonomické řešení SMS. SMS Pro Basic je určen pro provozovatele s omezeným rozpočtem, kteří potřebují jednoduchý SMS, s nímž se jednoduše

pracuje stylem "zaškrtněte políčko" pomocí jednoduchého, uživatelsky přívětivého nástroje systému řízení bezpečnosti, založeného na webovém rozhraní.

Třetí možností je PROFESSIONAL. SMS Pro Professional umožňuje operátorům, aby rozvíjeli svou ICOA SMS implementaci na nejvyšší úroveň. Provozovatelé, jenž využívají tento systém, musí uznat, že jim tento softwarový nástroj ušetří čas a úspory pracovních výhod tím, že jim maže neustále se opakující práce.

Poslední variantou je ENTERPRISE. SMS Pro Enterprise poskytuje neomezený prostor pro ukládání souborů aktivit SMS a přístup ke všem modulům SMS Pro. Na vyžádání je k této variantě k dispozici online školení pro celý personál organizace provozovatele. Tato poslední varianta Enterprise je již mnohem komplexnější než předchozí varianty a to se také odráží v její ceně. [17]

Software SMS Pro je placená služba. Dalo by se říct, že to, že se za používání tohoto systému platí měsíční paušální částky, je nevýhoda. To znamená, že si společnost nemůže tento software koupit a používat jej neomezeně, ale musí jistou částku zaplatit každý měsíc. Částky za tento software se liší podle varianty, kterou si společnost zvolí, a také podle počtu zaměstnanců ve společnosti. Náznak cenové nabídky společnosti NWDS je v následující tabulce. Výhodou však je, že software je neustále aktualizován a automaticky obsahuje nejnovější verzi programu, jak jej společnost NorthWest Data Solutions vyvíjí. Samozřejmě také obsahuje i nejnovější požadavky ze stran mezinárodních organizací obchodní letecké dopravy.

| Počet zaměstnanců | Starter | Basic | Professional | Enterprise |
|---|---|---|---|---|
| 1 až 20 | $50 | $75 | $100 | $499 |
| 21 až 40 | $75 | $199 | $299 | $999 |
| 41 až 60 | $100 | $299 | $499 | $1,499 |
| 61 až 80 | $150 | $499 | $799 | $1,999 |
| 81 až 100 | $199 | $799 | $999 | $2,499 |
| 101 až 200 | $249 | $999 | $1,199 | $3,299 |
| 201 až 300 | $299 | $1,199 | $1,399 | $4,499 |
| 301 až 500 | $349 | $1,299 | $1,599 | $6,999 |
| 501 až 750 | $499 | $1,599 | $1,999 | $8,999 |
| 751 až 1,000 | $799 | $1,999 | $2,499 | $9,999 |

*Tab. 6.: Ceník SMS Pro [17]*

## 7.2 AQD – Aviation Quality Database

Aviation Quality Database nabízí na trh společnost Teledyne Controls. Tato společnost byla již od roku 1964 dodavatelem sofistikovaných avionických výrobků a pozemních aplikací širokému spektru zákazníků civilního a vojenského letectví po celém světě. Teledyne Controls je přední poskytovatel řešení, jejichž cílem je pomáhat provozovatelům zvyšovat bezpečnost letu a provozní efektivitu prostřednictvím efektivnějších letových dat a řízení informací.

AQD je integrovaný systém řízení bezpečnosti, kvality a rizik, zahrnující všechny funkce od hlášení nehod/incidentů, řízení rizik, dodržování předpisů, analýzy a vyšetřování až po audity a sledování nápravných opatření. Software AQD byl vyvinut softwarovými leteckými odborníky a opírá se o 20 let zkušeností v poskytování softwarových řešení v oblasti letectví pro letecké úřady, letecké společností a další letecké organizace.

AQD je první systém, který kombinuje řízení jakosti s více tradičními koncepty bezpečnosti letů, aby systematicky zajistil, že nápravná opatření jsou účinná. Využitím osvědčeného přístupu k analýze příčin, viz obrázek níže, AQD shromažďuje zprávy o výskytu incidentů a nehod a spolu s interními a externími audity jakosti a bezpečnosti poskytuje organizaci široký pohled na problematiku bezpečnosti.

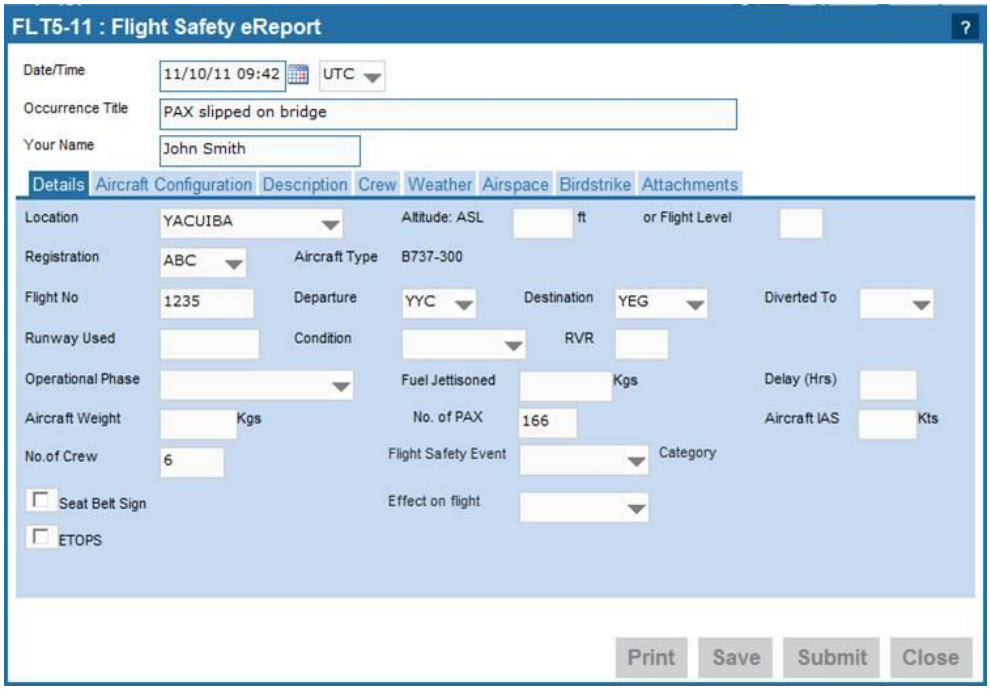

*Obr. 7.: James Reason model [18]*

AQD poskytuje snadný-k-použití, ale komplexní a efektivní nástroj pro správu procesů hodnocení rizik, analýzy, tvorby opatření, sledování a podávání zpráv pro dosažení požadovaného zlepšení výkonu. Z tvorby programu interních auditů, sledování nápravných opatření a integrací externích auditů, k analýze trendů v ukazatelích kvality, AQD pomáhá provozovatelům v souladu s JAR-OPS Řízení kvality a FAA Best Practice Requirements.

AQD používá řízení bezpečnosti a zásady řízení jakosti s cílem usnadnit cyklus neustálého zlepšování pomocí různých flexibilních a snadno použitelných nástrojů na podporu každé fáze procesu.

Sběr dat probíhá formou zachycení zpráv o incidentech/nehodách napříč všemi oblastmi organizace pro let, údržbu, bezpečnost práce ve vzduchu i na zemi s přihlédnutím na životní prostředí a další. Software pracuje prostřednictvím rozhraní přes prohlížeč pomocí přizpůsobitelných formulářů. Pro sběr dat mimo jiné používá také Flight Data Monitoring (FDM), což je systém zajišťující proces zajištění kvality, který se skládá ze stahování a analýzy dat z letadel na rutinní bázi. Jeho cílem je usnadnit nápravná opatření v rozsahu provozních oblastí, včetně bezpečnosti, provozu a údržby.

Na následujících obrázcích je možno vidět, jak software AQD pracuje. Záznamy o událostech jsou vytvářeny pomocí formulářů s nabídkou možností. Nabídka možností urychlí systém hlášení a také zajistí, aby hlášení obsahovalo všechny patřičné náležitosti. Formuláře se rozkládají na několika stránkách, kde lze zaznamenat všechny informace o události. Mezi hlavní detaily patří, co se vlastně stalo, následováno kde se to stalo, myšleno na jakém místě, dále jakého letadla se událost týče nebo za jakého počasí. Během sběru informací hrají všechny aspekty důležitou roli, aby v následující fázi bylo možné danou situaci vyšetřit a v budoucnu se podobné události vyhnout. Na následujícím obrázku vidíme, jak vypadá systém hlášení v systému AQD.



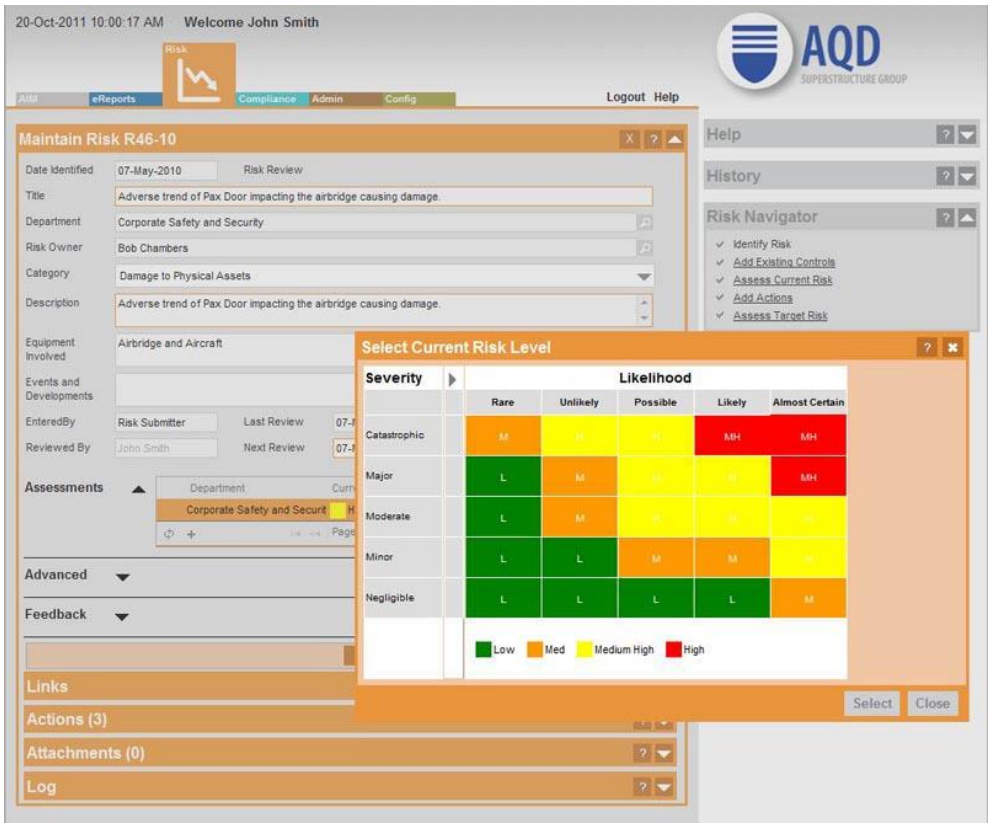

*Obr. 8.: Flight Safety eReport [18]*

Zaznamenaná hlášení o událostech jsou po jejím dokončení roztřízena a uložena do systému pro další zpracování. Zprávy jsou roztřízené do kategorií podle rozpracovanosti, to znamená, že zpráva není přijata, dokud nejsou doplněny všechny potřebné údaje, která zpráva musí

obsahovat pro další šetření. K vyplněným hlášením se tedy lze vracet a některé údaje doplňovat tak, aby vše bylo kompletní.

Zhodnocení dat probíhá za pomoci osvědčeného nástroje pro zhodnocení rizik a řízení vyšetřování a pomocí procesu auditů, záznamů z objektivních dat a poznatků. Zhodnocení zahrnuje zavedení modelů rizik a příčin k usnadnění identifikace kořenů příčin.

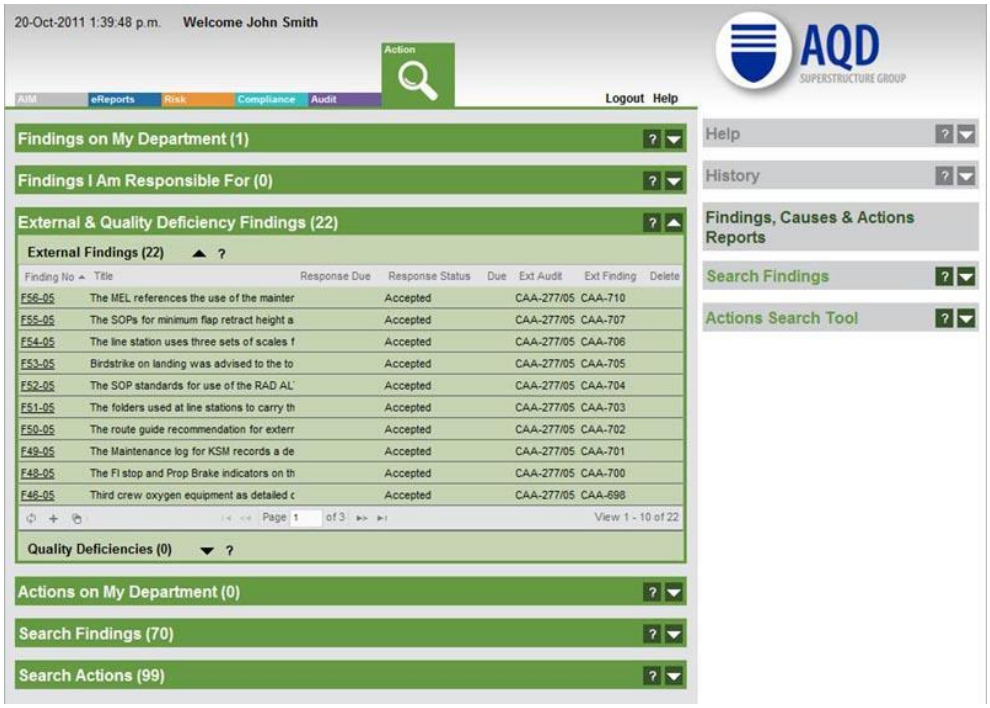
Proces vyhodnocení rizik probíhá podle modelu rozepsaného v předchozí kapitole. Tento proces počíná vlastním vyhodnocením události se zjištěním příčin dané události. Následujícím krokem je vyhodnocení možné pravděpodobnosti rizika, čímž se určí, jak je velká pravděpodobnost, že se stejná událost stane znova. Po zjištění pravděpodobnosti rizika se dále určuje klasifikace vážnosti rizika, díky tomuto faktoru je známo, jak velké škody s sebou tato událost přináší. Posledním krokem v tomto procesu je spojení těchto dvou faktorů do matice vyhodnocení rizik a vyhodnocení, zda je riziko nebezpečí nízké, střední, středně vysoké nebo vysoké. Vyhodnocení rizik spolu s maticí vyhodnocení rizik můžeme vidět na následujícím obrázku ze softwaru AQD.




*Obr. 9.: Hodnocení rizik [18]*

Nápravná a preventivní opatření řešení problémů jsou zjištěné pomocí řízení rizik, auditů a šetření na zmírnění rizika. Jejich realizace mohou pak být přesně řízeny a sledovány, aby se zajistilo, že výhody, jež byly zjištěny, jsou realizovány.

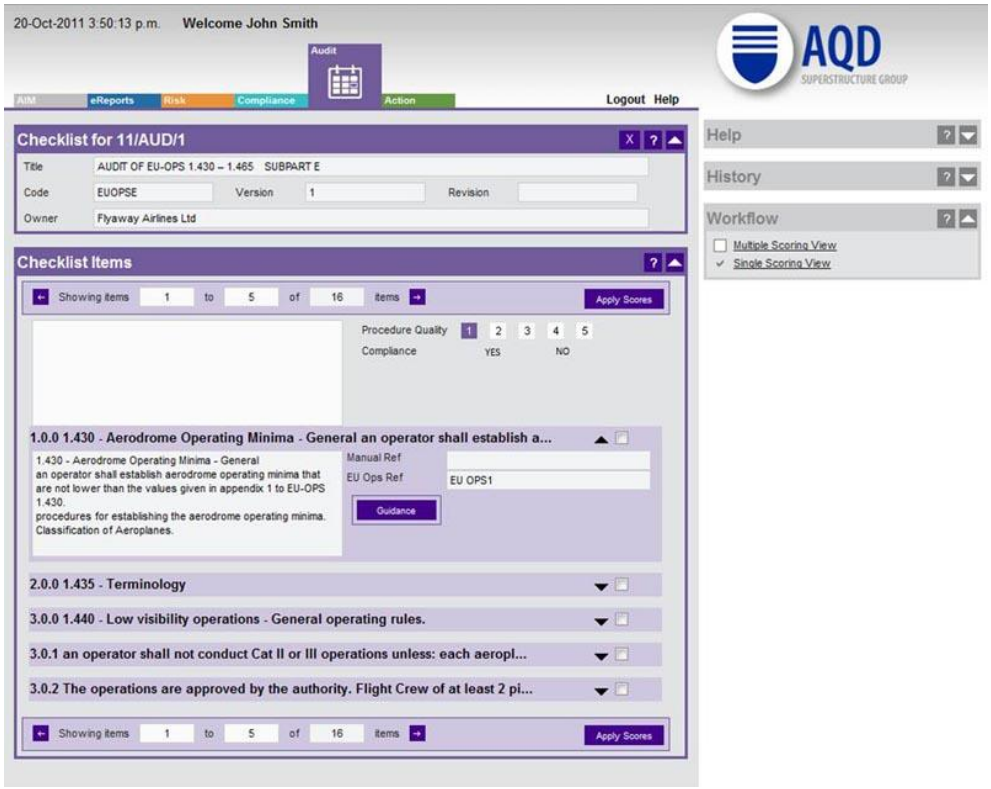
Sledování realizace nápravných opatření musí být jednoduché a musí být vždy jasné, zdali řešení problémů bylo správné a dostačující.




*Obr. 10.: Zprávy nálezů, příčin a akcí [18]*

Účinnost akcí a výsledných zdokonalení systému je stanovena prostřednictvím pokračujícího sledování, hodnocení a analýzy trendů pomocí různých flexibilních a snadno použitelných nástrojů. Proaktivní hodnocení a posouzení rizik a automatické upozornění e-mailem usnadňuje cyklus neustálého zlepšování a snižuje riziko v rámci celé organizace. [18]

Pro zajištění bezpečnosti v organizaci je zapotřebí, aby se celý předchozí cyklus neustále opakoval. Samozřejmě se musí reagovat na každé hlášení událostí od zaměstnanců a musí být co nejdříve vyřešeno. Důležitým prvkem však je neustálá kontrola systémů i mimo hlášení, která je zajištěna prováděním kontrol a auditů systému. Software AQD zahrnuje prvek, jenž automaticky vytvoří plán auditů pro danou organizaci na základě velikosti a složitosti organizace. Před blížícími se audity systém dává upozornění, kdy mají nastat. Ukázka plánu auditů v softwaru AQD je zobrazena na následujícím obrázku.




*Obr. 11.: Plán auditů [18]*

## 7.3 Q-Pulse

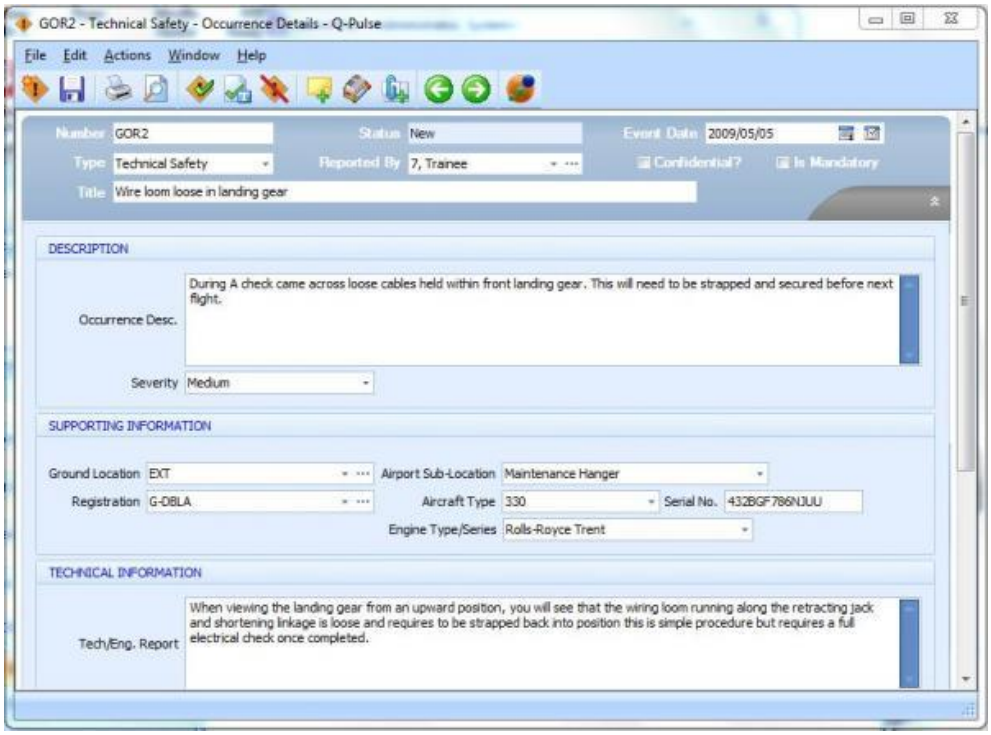
Software Q-Pulse vytváří a nabízí společnost Gael Ltd. Tato společnost Gael pomáhá od roku 1992 organizacím v mnoha odvětvích průmyslu zvládat řízení, dodržovat předpisy a rizika efektivněji a účinněji. Od roku 1999 je předním poskytovatelem softwaru pro řízení kvality, bezpečnosti a rizik v leteckém průmyslu. Jejich vizí je povzbudit společnosti, aby se zaměřily na to, co je důležité v jejich organizaci. V dnešní době používá jejich software více než dva a půl tisíce společní v 86 zemích světa a v letectví používá software Q-Pulse více než tři sta leteckých společností. [19, 20]

Software Q-Pulse je založen na čtyřech základních komponentech, které obsahuje a které by měl obsahovat každý efektivní systém řízení bezpečnosti.

První z těchto komponent je zabezpečení jakosti a bezpečnosti. To nám říká, že systém řízení bezpečnosti by měl obsahovat klíčové prvky řízení kvality. Mezi tyto prvky patří především řízení auditů, správu dokumentů a nápravná neboli preventivní opatření. Díky začlenění těchto prvků do SMS vznikají lepší výkony v oblasti bezpečnosti.

Další důležitou součástí softwaru Q-Pulse je systém pro hlášení incidentů. Proto, aby zprávy zachycovaly podstatu incidentu a sesbíraly všechny potřebné informace důležité pro další šetření rizik, je sběr zajištěn pomocí formulářů s povinnými poli a nabídkou z rozevíracích seznamů. Formuláře mohou být nakonfigurovány tak, aby spravovaly více typů událostí, jako jsou střety s ptáky, TCAS, hlášení letových posádek, palubních průvodčí, pracovníku handling, důvěrné zprávy a podobně. Výhodou tohoto dělení hlášení podle typu je, že systém automaticky rozešle hlášení na e-mail všem osobám, kterých se daná problematika týče a dále je pak průběžně seznamuje s postupem šetření události. Systém je navíc přístupný prostřednictvím počítače nebo IPadu a nabízí taky napojení na Flight Data Monitoring.

Ukázku jak může vypadat rozhraní pro hlášení incidentů/nehod můžeme vidět na dalším obrázku. Na něm je vidět, že formulář hlášení má několik částí, z nichž jedna je část s nabídkou rozevíracích možností, která se týká specifikací události. Mezi tyto údaje patří typ zprávy, jak je napsáno výše, číslo události, kdo událost napsal a datum kdy se to vlastně odehrálo. Mezi další specifikace patří okolnosti události, upřesnění místa události a letadla, kterého se to týče. Dalšími částmi jsou textová pole pro podrobný popis situace, v nichž jsou informace, jenž slouží pro další operace při řízení bezpečnosti.

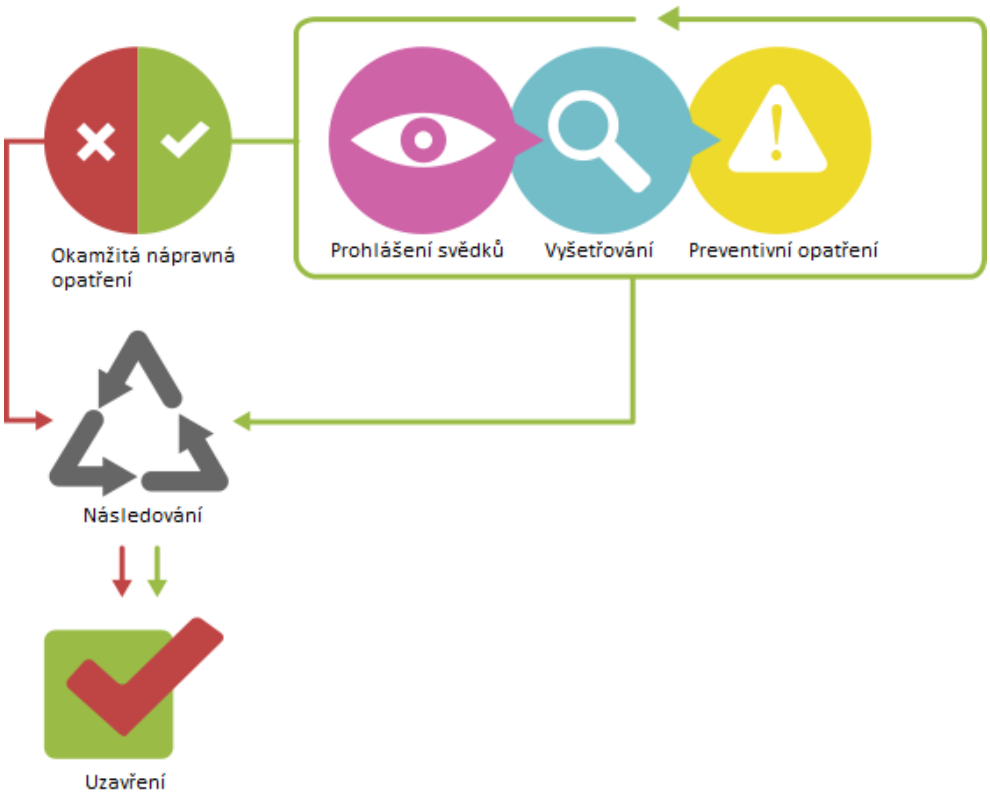



*Obr. 12.: Systém hlášení [22]*

Vyšetřování a analýza dostupných hlášení začíná automatickým přezkumem, kde se zjistí, zda je zpráva kompletní a zda je potřeba zajistit další kroky, jako je získat další informace,

nepodnikat nic nebo přejít k vyšetřování. Pokud je tedy hlášení v pořádku odesláno, začíná na jejím podkladu šetření události a identifikace nebezpečí, aby se zjistilo, kvůli čemu vlastně k události došlo.

Dále se přezkoumává, za pomocí řízení rizik, zda jsou nutné změny ke snížení rizika do budoucnosti. Analýza dat zachycených prostřednictvím zpráv je prospěšná v oblasti řízení změn v celé organizaci. Nesmí dojít k vyvozování následků pouze z předpokladu. Důležité je celou událost pořádně vyřešit a až na základě zjištěného rizika vyvozovat závěry. Správné vyšetřování hlášení by mělo postupovat podle schématu softwaru Q-Pulse uvedeného na následujícím schématu.




*Obr. 13.: Analýza hlášení [19]*

Posledním komponentem podle struktury Q-Pulse je měření výkonnosti. Neustálým přezkoumáváním důkazů předložených prostřednictvím zpráv a auditů umožní organizaci monitorovat jejich výkonnost oproti předem definovaným parametrům. Mohou snadno určit, kdy se věci začínají kazit, a mohou řešit případné problémy dříve, než se stávají velkým problémem.

Zavedením efektivního systému řízení bezpečnosti na základě výše uvedených složek budou moci organizace kvantifikovat jako výnos z jejich investice následující:

- Informovanější rozhodování
- Vylepšená bezpečnost pomocí efektivního řízení rizik
- Umožněná lepší alokace zdrojů, což vede ke zvýšení efektivnosti a snížení nákladů
- Vytvoření otevřené firemní kultury, která podporuje hlášení
- Prokazatelná náležitá péče

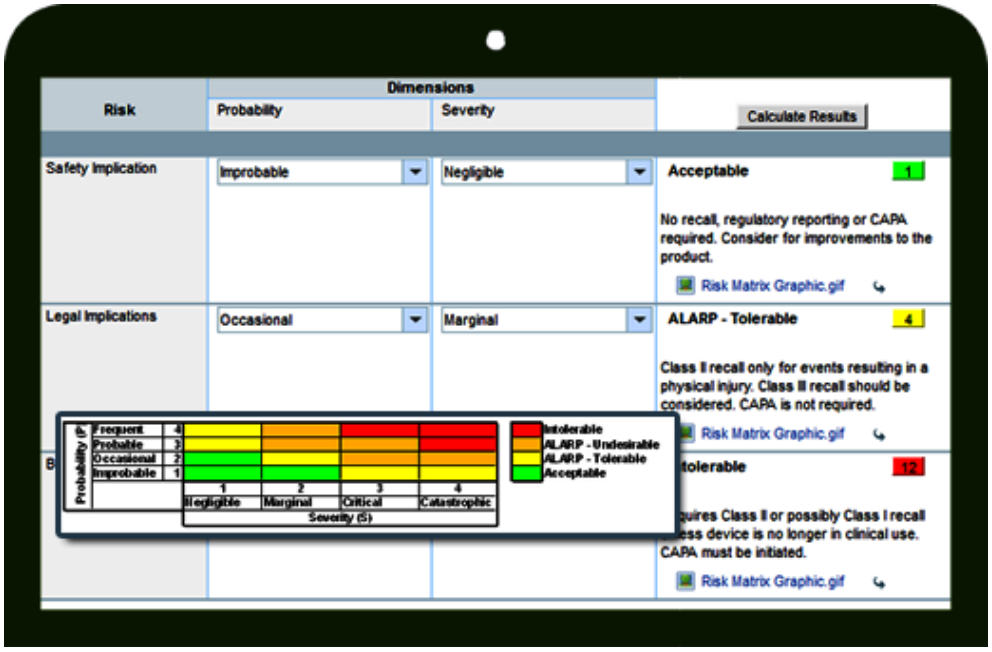
Řešení SMS pomocí Q-Pulse využívá řízení kvality s cílem zajistit úplný soulad k regulaci a schopnost prokázat shodu úřadům, klientům a auditorům. [19]

## 7.4 EtQ

Společnost EtQ Inc. byla založena roku 1992 a využívá principy ověřené více než dvacetiletými zkušenostmi v oblasti podnikových softwarových aplikací a v oblasti řízení shody. V dnešní době má společnost více než 500 zákazníků. Zakladatelé EtQ jsou inženýři a obchodníci, kteří věří, že budoucnost funkčnosti podnikových aplikací bude v rukou obchodních uživatelů. Vývoj aplikací technologie EtQ umožňuje uživatelům vytvářet, konfigurovat a personalizovat výkonné aplikace firmy.

Prostřednictvím EtQ, jsou uživatelé schopni nastavit všechny aspekty řešení - pracovní postupy, formuláře, pole, klíčová slova - vše konfigurovatelné bez nutnosti programování. To umožní společnosti přizpůsobit řešení procesům a snadno se přizpůsobit jakékoli změně.

Bezpečnost je cíl, to je důvod, proč systém řízení bezpečnosti od EtQ poskytuje zobrazení bezpečnostních hlášení událostí a umožňuje přijmout okamžitá opatření v souladu s dodržováním předpisů. EtQ vyvinula robustní inteligentní platformu hlášení, postavenou přímo do systému. Používáním grafů, pohledů a upozorněním na hlášení a zprávy mohou uživatelé zvýšit viditelnost veškerých dat a činit informovanější rozhodnutí také díky automatickému roztřízení zpráv, automatickému zobrazení souvisejících zpráv a díky vestavěné bezpečnostní analýze rizik. EtQ je průkopníkem koncepce řízení operačního rizika v oblasti řešení pro dodržování předpisů, a vybudovala kvantitativní nástroje pro podporu řízení rizik. Nástroje pro řízení rizik jsou postaveny tak, aby umožňovaly vytvářet šablony rizik a nakonfigurovat je do jakéhokoli procesu. Vytvořením rizikové matice se automaticky vypočítá riziko, začlení do rozhodovacího stromu a přidává filtry rizik.




*Obr. 14.: Řízení rizik [20]*

Integrovaný systém řízení bezpečnosti EtQ poskytuje uzavřený proces zaznamenávání a podávání zpráv o životním prostředí, zdraví a bezpečnostních událostech v rámci systému. Unikátní systém řízení bezpečnosti je navržen tak, aby prioritou bylo minimalizovat počet vysoce rizikových událostí pomocí pokročilého modelu filtrování na základě řízení rizik. Tento systém automaticky segreguje a třídí události u zdroje, používá kvantitativní hodnocení rizik v průběhu celého procesu, vede rozhodování a nabízí komplexní program nápravného opatření a efektivity kontrolního plánu s historií snižování rizika. EtQ využívá přes dvacet ve své třídě nejlepších integrovaných modulů a integraci podnikových aplikací pro správu a měření kvality a dodržování procesů a provádění organizačních změn. Mezi zmiňované moduly patří například kontrola dokumentů, řízení auditů, analýza bezpečnosti, nápravná opatření, řízení změn, bezpečnostní hlášení, školení zaměstnanců a podobně. [20]

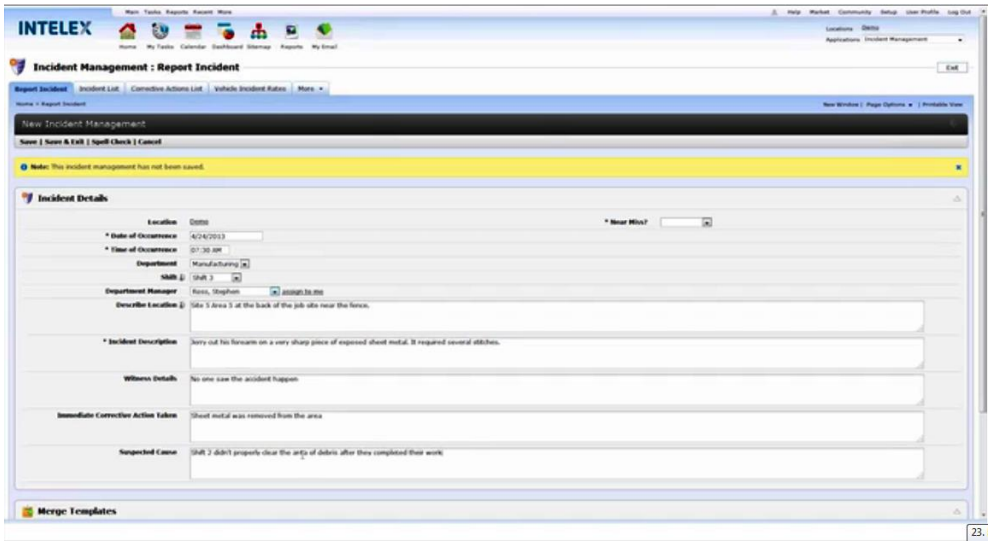
## 7.5 Intelex

Společnost Intelex byla založena roku 1992 a od svého založení se zabývá vývojem a realizací softwaru pro ochranu životního prostředí a systémy pro řízení bezpečnosti a kvality. Společnost využívá nejnovější technologie proto, aby se svět stal lepším a bezpečnějším místem. V dnešní době je společnost Intelex světová jednička ve vývoji EHS (Environment, Health, Safety) a softwaru pro řízení kvality, nejstarší nezávislý dodavatel EHS a softwaru pro řízení kvality v Severní Americe a jedna z největších kanadských softwarových společností.

Intelex vyvíjí, implementuje a podporuje software pro ochranu životního prostředí, zdraví a řízení bezpečnosti a kvality po více než dvacet let. Jejich celosvětová klientská základna s více než 1000 zákazníků a 1 milionem uživatelů systému je závislá na jejich softwaru, jenž zachycuje, sleduje a informuje uživatele o zásadních datech jejich podniku.

Pro letecké společnosti je prvořadá bezpečnost cestujících a posádky. Intelex sestavil řešení systému řízení bezpečnosti (SMS) pro letecké společnosti po celém světě ve webovém rozhraní, které se zaměřuje na počty nehod/incidentů, audity, školení, hodnocení rizik v reálném čase a další vzdušné a pozemní procesy související s bezpečností. Všechna řešení splňují požadavky letové integrace dat a komunikace přímo s letovými datovými systémy.

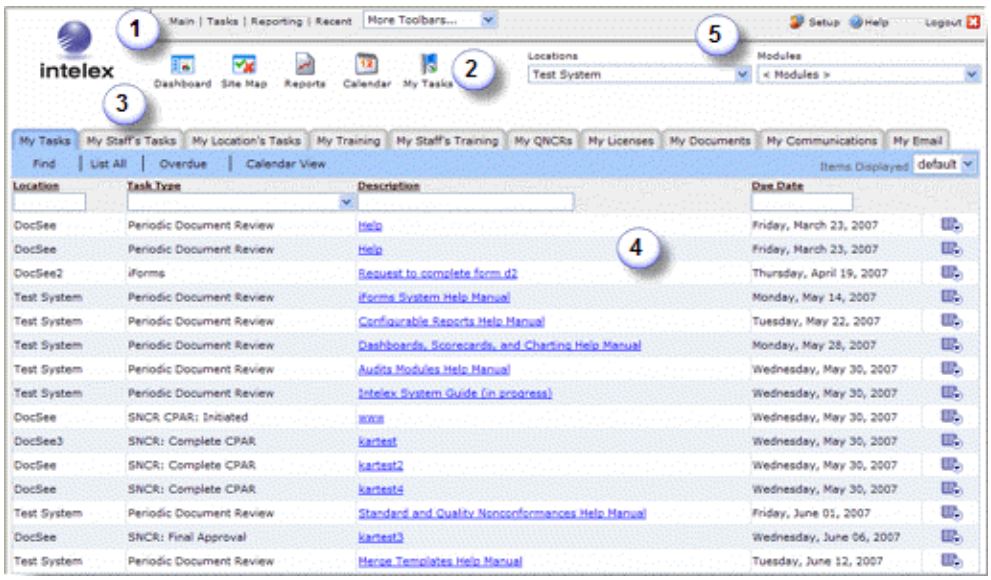
Každý nainstalovaný SMS má možnost zachovat jednu z mnoha plně konfigurovatelných forem hlášení incidentů. Společnost se může rozhodnout, zda bude uchovávat všechna hlášení v jediné dynamické formě, nebo nakonfigurovat několik samostatných formulářů pro zpracování letecké bezpečnosti, pro pozemní výskyty bezpečnostních incidentů atd. Hlavní formulář je stejný pro všechny formy, obsahuje totiž základní informace a místu a času incidentu, jenž se vyplňuje pomocí rozevíracích nabídek, což urychluje hlášení a usnadňuje automatické roztřízení hlášení podle nabízených možností. Ukázku systému hlášení softwaru Intelex můžeme vidět na následujícím obrázku.




*Obr. 15.: Systém hlášení [21]*

Řízení rizik může čerpat z centralizovaného hodnocení rizik, kterým umožňuje SMS definovat rizikové skóre pro jakýkoliv záznam z konfigurovatelného, ale standardizovaného nástroje pro posouzení rizik. To urychluje celý proces řízení bezpečnosti, protože se vychází z již vyhodnocených podobných nebo stejných událostí, a není potřeba celým procesem procházet neustále od počátku.

Nakonfigurovaný SMS má také schopnost dodržovat uživatelem definované termíny kontrol nařízených předpisy. Systém totiž obsahuje modul se seznamem nadcházejících úkolů, jako jsou kontroly, interní nebo externí audity. V seznamu jsou navíc i záznamy o již vykonaných auditech i se závěrečnými zprávami a hodnoceními systému. Díky zprávám a hodnocením auditů se snadno stanovuje výkonnost celého systému a zjišťuje se, zda je systém efektivní.




*Obr. 16.: Seznam úkolů [21]*

Mezi klíčové komponenty a funkce SMS společnosti Intelex patří:

- Správa auditů
- Školení managementu
- Hlášení událostí, nehod a nebezpečných stavů
- Řízení nebezpečí a rizik
- Analýza kořene příčin a řízení nápravných opatření. [21]

# 8 MODELOVÁ APLIKACE

Jedním z bodů zadání této práce je provést modelovou aplikaci softwarových nástrojů na organizaci pro výcvik (ATO) se složitou organizací. Za složité ATO se považují mimo jiné organizace, které poskytují výcvik k získání CPL nebo pro získání nebo rozšíření instruktorských kvalifikací podle dokumentu CAA-ZLP-141 Organizace pro výcvik v létání.

Pro modelovou aplikaci pro tuto práci jsem si zvolil organizaci poskytující výcviky PPL(A), CPL(A) a NIGHT(A). Organizace je složena celkově z osmi osob, z nichž každý zastává svou funkci.

První důležitou osobou je odpovědný vedoucí, ten stojí v čele ATO a je jednatelem organizace. Další osobou je vedoucí výcviku, který je přímo podřízený odpovědnému vedoucímu, má celkovou zodpovědnost za dodržování postupů výcviků dle Part-FCL, za skloubení teoretické a praktické výuky a za hodnocení odborné způsobilosti jednotlivých uchazečů o zkoušku dovedností. Mezi další osoby v organizaci patří také vedoucí letový instruktor, ten je plně podřízen vedoucímu výcviku a sám nese odpovědnost i za dohled nad letovými instruktory. Standardizaci a dohled může vedoucí letový instruktor delegovat na letové instruktory, ale sám nese konečnou odpovědnost za jejich zajištění. Další důležitou osobou v organizaci je vedoucí instruktor teoretické výuky, ten nese zodpovědnost za dodržování jednotné osnovy a za materiály pro teoretickou výuku a odpovídá za všechny instruktory teoretické výuky. Kromě všech výše uvedených zaměstnanců organizace má další tři instruktory vykonávající funkce praktického i teoretického výcviku. [23]

Mezi další důležité funkce v organizaci patří vedoucí bezpečnosti, ten musí mít dobrou znalost systému řízení bezpečnosti, techniky auditování, provozních předpisů a dokumentace ATO. Mezi jeho povinnosti patří odpovědnost za *„tvorbu, administraci a udržování SMS ATO, usnadňování identifikace nebezpečí a rizik, sledování opatření pro zmírnění rizik podle akčního plánu bezpečnosti, podávání pravidelných hlášení odpovědnému vedoucímu o výkonnosti SMS, vedení dokumentace o řízení bezpečnosti, zajišťování dostupnosti výcviku řízení bezpečnosti a jeho přijatelnou úroveň, poskytování poradenství v oblasti bezpečnosti a zajištění zahájení interního šetření událostí a následnou reakci na jeho výsledky.“ [23]*

Poslední osobou v této organizaci je vedoucí sledování shody, ten má mít dobrou znalost systému řízení bezpečnosti, techniky auditování, provozních předpisů a dokumentace ATO a zkušenosti se sledováním shody. Musí mít přímý přístup k odpovědnému vedoucímu, do všech částí ATO a případně i do smluvních organizací. [23]

## 8.1 Politika a záměry/cíle bezpečnosti

Během procesu zavádění systému řízení bezpečnosti je důležité mít jednotlivé kroky pořádně rozplánovány, aby se na některé oblasti nezapomnělo. Prvním krokem v organizaci však je určení politiky a záměrů/cílů bezpečnosti. Do této fáze hlavně spadá úkol odpovědného vedoucího definovat bezpečnostní politiku organizace a jmenování vedoucího bezpečnosti a členů výboru pro přezkoumávání bezpečnosti. Vedoucí bezpečnosti má dále zodpovědnost za všechny kroky podniknuté v implementaci SMS, včetně koordinace plánu reakce na nouzové situace a vytvoření SMS dokumentace.

Podle těchto požadavků a jejich přesnějších specifikací v předchozích kapitolách pro tuto činnost vyhovují všechny zmíněné softwarové produkty, jež jsou popsány výše. Všechny produkty obsahují ve svém menu záložku, ve které jsou krok po kroku vypsány jednotlivé činnosti, které je potřeba během celé implementace vykonat, a především v softwaru SMS Pro jsou zde i zvýrazněné kroky, které již jsou vykonané a vše je velmi přehledné.

## 8.2 Řízení bezpečnostního rizika

Řízení bezpečnostního rizika je založeno na několika procesech. První z nich je zjišťování nebezpečí v organizaci. Tato činnost je ve všech představených nástrojích zajištěna výbornými systémy hlášení, řízením programů auditů a např. u nástrojů AQD a Q-Pulse je systém doplněn o automaticky přidávané záznamy a hlášení ze systému flight data monitoring. Systémy hlášení jsou u všech softwarových nástrojů propracovány a usnadňují vytváření hlášení pomocí rozevíracích seznamů s nabídkou rychlých odpovědí na základní údaje formuláře.

Dalším procesem je proces vyhodnocení a zmírnění rizika. Tento proces začíná vyhodnocením rizika, pro tuto činnost má každý z uvedených softwarů jiné nástroje. Například nástroj společnosti Intelex připojí k hlášení informace z různých zdrojů i mimo organizaci provozovatele, za účelem porovnání incidentu a pro rychlejší a snadnější zhodnocení rizik. Všechny nástroje používají pro hodnocení rizika matici vyhodnocení rizik, která rozhoduje, jestli je riziko přijatelné, snesitelné nebo nepřijatelné. Na základě vyhodnocení maticí rizik se přistupuje k jeho zmírňování, pokud je to potřeba.

## 8.3 Ověřování úrovně bezpečnosti

Na systém řízení bezpečnostního má také značný vliv ověřování úrovně bezpečnosti. Úroveň bezpečnosti se v organizaci ověřuje pomocí sledování výkonnosti v bezpečnosti. Tato činnost se skládá z bezpečnostních hlášení, studií, posuzování, auditů a průzkumů dotazováním.

Všechny výše uvedené softwarové nástroje tyto činnosti umožňují a mají pro ně vytvořené vlastní prostředí. Bezpečnostní studie a audity ve společnosti jsou vykonávány podle rozpisu jak interními, tak externími auditory.

## 8.4 Podpora bezpečnosti

Podpora bezpečnosti je v organizaci zajištěna především systémem bezpečnostních výcviků. Bezpečnostní výcviky musí absolvovat všichni zaměstnanci počínaje vrcholovým vedením. V systému řízení bezpečnosti by měli mít všichni zaměstnanci organizace vlastní složku, kde je sepsáno, jaké výcviky podstoupili, a kdy a jaký obnovovací výcvik zaměřený na bezpečnost by měl následovat. Všechny výše uvedené softwarové nástroje takový přístup umožňují a mají pro něj připravený modul, který na takováto školení včas upozorňuje, podle stanoveného plánu.

Pro zajištění podpory bezpečnosti musí v organizaci fungovat bezpečnostní komunikace. Ve všech nástrojích je vhodná služba pro rozesílání e-mailů zaměstnancům s důležitými informacemi o fungování organizace. Kromě toho by ve společnosti měla fungovat komunikace formou schůzí a porad, kde by se měly otázky bezpečnosti řešit v přátelském duchu v otevřené konverzaci.

Na závěr této kapitoly je potřeba říci, že všechny nástroje, popsané v předchozí kapitole, jsou vhodnými a plnohodnotnými softwarovými nástroji pro podporu safety management systému v letectví.

# ZÁVĚR

Cílem této práce bylo identifikovat softwarové nástroje, jež by usnadnily implementaci systému řízení bezpečnosti.

V první části této práce jsem se zabýval seznámením s pojmy jako bezpečnost nebo systém řízení bezpečnosti, co jej ovlivňuje a jaké jsou přístupy k jeho řízení.

Nedílnou součásti tohoto tématu je také seznámení se s historií problematiky řízení bezpečnosti. Touto otázkou jsem se zabýval v následujících kapitolách. První z nich byla kapitola dokumentující předpisy a další dokumenty, které se zabývají otázkou řízení bezpečnosti. Zde jsem se dozvěděl, které státní i nestátní organizace se tímto problémem zabývají. Jednotlivé organizace k tomuto problému, řízení bezpečnosti, vydaly i své předpisy, doplněné o jednotlivé průvodní dokumenty a manuály. U nás v České republice se také objevily přeložené předpisy, kterými je třeba se řídit. Další kapitolou je přímo historie vývoje řízení bezpečnosti. V této kapitole jsem si rozdělil minulost na tři období, ve kterých se řízení bezpečnosti postupně zabývalo jinou otázkou bezpečnosti letectví, přičemž poslední období přetrvává do dnešní doby.

Bezpečnostní kultura organizace provozovatele je samozřejmě také důležitý parametr. Důležitým poznatkem zde je upozornění na ohlašovací systémy a jak by měly fungovat. Fakt, že bezpečnostní kultura závisí především na vrcholovém vedení a jejím přístupu k řízení bezpečnosti, je důležitý. Poněvadž pokud neprojeví o systém řízení bezpečnosti zájem vrcholové vedení a nebude mu věnovat dostatek času a prostředků, tak bude v organizaci na velice nízké úrovni.

Všeobecné znalosti o systému řízení bezpečnosti nás přivedly až k samotné struktuře implementace safety management systému. V této kapitole jsem se dozvěděl, že implementace má zahrnovat čtyři základní komponenty. Mezi tyto komponenty patří politika a cíle společnosti, řízení bezpečnostního rizika, ověřování úrovně bezpečnosti a podpora bezpečnosti. Jednotlivé komponenty jsou rozepsány v kapitole výše a provedly tak čtenáře celým procesem implementace systému řízení bezpečnosti.

Po předchozích kapitolách, ve kterých jsem se dozvěděl vše o systému řízení bezpečnosti a o komponentech důležitých pro implementaci systému, jsem se dostal až ke stěžejní části práce. V této části jsem se dozvěděl, jaké existují na trhu softwarové nástroje pro usnadnění implementace a jaké mají vlastnosti.

Posledním bodem této práce byla modelová aplikace zvolených nástrojů na složitou organizaci pro výcvik.

# SEZNAM POUŽITÉ LITERATURY


1. *Letiště Praha, a. s.. Safety Management Systém. 2015. Dostupné na: http://www.prg.aero/cs/o-letisti-praha/bezpecnost-na-letisti/safety/safety-management/*

2. *VLČEK, F. Směrnice CAA-FOD-01/2013: Poradní materiál k požadavku ORO.GEN.200 systém řízení. 2013. 103 s.* [cit. 21. 01. 2015]. *Dostupné na: http://www.caa.cz/file/6472*

3. *VŠB-TU Ostrava. Fakulta strojní. Kapitola I. Lidský činitel v letecké dopravě. 2009.* [cit. 21. 01. 2015]. *Dostupné na: http://projekt150.ha-vel.cz/node/117*

4. *VANOUREK, J. Lidský faktor v letectví. Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2009. 81 s. Vedoucí diplomové práce Ing. Miroslav Šplíchal, Ph.D.*

5. *NAJMAN, Jan. Privatizace mezinárodních letišť v České republice a její bezpečnostní aspekty. 2012. Bakalářská práce. Masarykova univerzita, Fakulta sociálních studií. Vedoucí práce Miroslav Mareš.*

6. *TALBOT, J., High Technology Estate. ALARP (As Low As Reasonably Practicable).* [cit. 21. 01. 2015]. *Dostupné na: http://www.jakeman.com.au/media/alarp-as-low-as-reasonably-practicable*

7. *ŠALANDA, M. Zavedení systému řízení bezpečnosti u malého leteckého dopravce. Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2008. 58 s. Vedoucí diplomové práce Ing. Ondřej Schaumann.*

8. *MOKOŠ, M. Vliv připravovaného ICAO Annex 19 na letecké provozovatele v ČR. Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2013. 61 s. Vedoucí diplomové práce Ing. Jiří Chlebek, Ph.D.*

9. *MINISTERSTVO DOPRAVY ČR. L 19 Řízení bezpečnosti. 166/2013-220-LPR/1. Praha: LIS, 2013.* [cit. 26. 02. 2015]. *Dostupné na: http://lis.rlp.cz/predpisy/predpisy/index.htm*

10. *ICAO: Safety Management Manual (SMM). Doc. 9859, Montreal, 2006*

11. *EVROPSKÁ KOMISE, Nařízení komise (EU) č. 965/2012 ze dne 5. října 2012, kterým se stanoví technické požadavky a správní postupy týkající se letového provozu podle nařízení Evropského parlamentu a Rady (ES) č. 216/2008. Brusel: 2012*

12. *EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE. Nařízení evropského parlamentu a rady (ES) č. 216/2008 ze dne 20. února 2008 o společných pravidlech v oblasti civilního letectví a o zřízení Evropské agentury pro bezpečnost letectví, kterým se ruší směrnice Rady 91/670 EHS, nařízení (ES) č. 1592/2002 a směrnice 2004/36/ES. Štrasburk: 2008*

13. *MINISTRSTVO DOPRAVY ČR. L6 Provoz letadel. 35/2012-220-SP/2. Praha: LIS, 2012.* [cit. 26. 03. 2015]. *Dostupné na: http://lis.rlp.cz/predpisy/predpisy/index.htm*

14. *MINISTERSTVO DOPRAVY ČR. L11 Letové provozní služby. 25345/99-220. Praha: LIS, 2014.* [cit. 26. 03. 2015]. *Dostupné na: http://lis.rlp.cz/predpisy/predpisy/index.htm*

15. *MINISTERSTVO DOPRAVY ČR. L14 Letiště. 439/2005-220-SP/1. Praha: LIS, 2011.* [cit. 26. 03. 2015]. *Dostupné na: http://lis.rlp.cz/predpisy/predpisy/index.htm*

16. *INTERNATIONAL AIR TRANSPORT ASSOCIATION. Safety report 2014. ISBN 978-92-9252-582-8. Montreal—Geneva. 2015.*

17. *SMS Pro* [online]. *Dostupné na: http://www.asms-pro.com*

18. *Teledyne Controls* [online]. *Dostupné na: http://www.teledynecontrols.com*

19. *Gael-quality* [online]. *Dostupné na: http://www.gaelquality.com*

20. *Q-Pulse*[online]. *Dostupné na: http://www.q-pulse.com*

21. *Intelex* [online]. *Dostupné na: http://www.intelex.com*

22. *MaXsimise Aerospace (Pty) Ltd* [online]. *Dostupné na: http://www.maxsimiseaerospace.co.za*

23. *ÚŘAD PRO CIVILNÍ LETECTVÍ. Organizace pro výcvik v létání. CAA-ZLP-141. 2015. [cit. 04. 02. 2013]. Dostupné na internetu: http://www.caa.cz/file/7696/*

# SEZNAM OBRÁZKŮ

*Obr. 1.: ALARP*

*Obr. 2.: SHELL*

*Obr. 3.: Reasonův model*

*Obr. 4.: Vývoj Bezpečnosti*

*Obr. 5.: SMS implementation plan*

*Obr. 6.: Classification report*

*Obr. 7.: James Reason model*

*Obr. 8.: Flight Safety eReport*

*Obr. 9.: Hodnocení rizik*

*Obr. 10.: Zprávy nálezů, příčin a akcí*

*Obr. 11.: Plán auditů*

*Obr. 12.: Systém hlášení*

*Obr. 13.: Analýza hlášení*

*Obr. 14.: Řízení rizik*

*Obr. 15.: Systém hlášení*

*Obr. 16.: Seznam úkolů*

## SEZNAM TABULEK

*Tab. 1.: Druhy bezpečnostní kultury*

*Tab. 2.: Klasifikace možné pravděpodobnosti rizika*

*Tab. 3.: Klasifikace vážnosti rizika*

*Tab. 4.: Matice vyhodnocení rizika*

*Tab. 5.: Bezpečnostní SMS výcviky*

*Tab. 6.: Ceník SMS Pro*